Appendix A-Executive Order 69 (2004)

Virginia's Secure Commonwealth Initiative

Among the most important responsibilities and profound duties of government at all levels is to provide for the safety and security of its citizens. With this most serious obligation in mind and by virtue of the authority vested in me by Article 5, Sections 1 and 7 of the Constitution of Virginia and by Section 44-146.17 of the Code of Virginia, I hereby establish the Virginia 's Secure Commonwealth Initiative. The purpose of this Initiative shall be to implement strategies that enhance the safety and security of the citizens of the Commonwealth. The Initiative shall include, but not be limited to, enhancing the Commonwealth's prevention, preparedness and response and recovery capability for natural disasters and emergencies of all kinds, including terrorist attacks.

Secure Commonwealth Panel

To support this Initiative, I hereby establish the Secure Commonwealth Panel (herein called the "Panel") to monitor and assess the implementation of statewide prevention, response and recovery initiatives and where necessary to review, evaluate and make recommendations relating to the emergency preparedness of government at all levels in the Commonwealth. Additionally, the Panel shall facilitate cabinet-level coordination among the various agencies of state government related to emergency preparedness and will facilitate private sector preparedness and communication. The Panel shall deliver to me by December 1, 2005, a comprehensive strategic plan that outlines the status of on-going statewide efforts and recommendations for future activities to manage the physical, economic and societal risks of emergencies and disasters of all kinds, including terrorism.

The Panel shall consist of 20 members. The chairman of the Panel shall be the Assistant to the Governor for Commonwealth Preparedness. Other members of the Panel shall include the Lieutenant Governor; the Attorney General; two members of the House of Delegates; two members of the Senate of Virginia; and the Secretaries of Health and Human Resources, Public Safety, Technology, and Transportation. The Governor shall appoint two local first responders and three local government representatives to the panel. The Governor shall also appoint four additional members from the private sector. Ex officio members may be appointed to the Panel by the Governor at his discretion.

Members of the Panel shall serve without compensation but may receive reimbursement for expenses incurred in the discharge of their official duties upon approval by the Governor's Chief of Staff or his designee. The Panel shall convene, within sixty days of the signing of this order.

The Panel shall prepare quarterly reports for the Governor to keep him apprised of the state's emergency preparedness, response, recovery and prevention efforts. Staff support for the Panel will be provided by the Office of the Governor, the Office of the Secretary of Public Safety, the Office of the Secretary of Health and Human Resources, the Department of State Police, the Department of Emergency Management, the Department of Planning and Budget, and such other executive offices and agencies as may be designated by the Governor. An estimated 500 hours of staff time will be required to support the work of the Panel.

Funding necessary to support the Panel's work will be provided from sources, including both private and appropriated funds, contributed or appropriated for purposes related to the work of the Panel, as authorized by Section 2.2-135(B) of the Code of Virginia. Direct expenditures for the Panel's work are estimated to be $60,000. All or part of the costs incurred by the Panel may be paid, upon my approval, out of the sum sufficient appropriation for Disaster Planning and Operations contained in Item 45 of Chapter 1073, 2000 Virginia Acts of Assembly, or any other funds available for such purpose.

State Agency Plans

I hereby direct all executive branch agency heads to certify to me by June 1, 2004 that they have completed updates and/or development of plans that address continuity of their operations and services, and the security of their customers and employees, in the event of natural or man-made disasters or emergencies, including terrorist attacks. I further direct that all executive branch agencies exercise and test these plans on or before September 1, 2005.

Responsibility for Homeland Security Issues

I hereby designate the Assistant to the Governor for Commonwealth Preparedness as my primary liaison for the U.S. Department of Homeland Security and the Executive Office of the President, Homeland Security Council. He shall be responsible for coordinating, on my behalf, activities as required to promote unity of effort among federal, state, local, private sector and citizen activities related to preparedness and homeland security.

I hereby designate the Secretary of Public Safety as the single point of contact for federal law enforcement agencies regarding homeland security issues and to serve as an alternate liaison to the U.S. Department of Homeland Security and Executive Office of the President, Homeland Security Council if so required.

I hereby designate the Assistant to the Governor for Commonwealth Preparedness to work with appropriate cabinet secretaries to coordinate grants that may be provided to improve preparedness in Virginia communities with the goal of ensuring an integrated enterprise wide approach to prevention and preparedness.

This Executive Order rescinds Executive Order 07 (02). Given under my hand and under the Seal of the Commonwealth of Virginia, this 3rd day of May 2004.

/S/ Mark R. Warner, Governor

Appendix B-Secure Commonwealth Panel Members

Jeffrey P. Bialos
Partner, Corporate
Sutherland Asbill & Brennan LLP
McLean, VA

Dr. Vinton G. Cerf
Senior VP, Technology Strategy
MCI
Ashburn, VA

BG (Ret.) Manuel R. Flores
State Director
Selective Service System
Chester, VA

George W. Foresman
Assistant to the Governor
Commonwealth Preparedness
Richmond, VA

Kay C. Goss
Senior Advisor for Homeland Security
Business Continuity and Emergency
Management Services
Electronic Data Systems Corp. (EDS)
Alexandria, VA

The Hon. Katherine K. Hanley
Former Chairman, Fairfax County
Board of Supervisors
Reston, VA

The Hon. Leroy Hassell
Supreme Court Chief Justice
Supreme Court of VA
Richmond, VA

The Hon. Pierce Homer
Secretary of Transportation
Richmond, VA

The Hon. Frank W. Horton
Former Chairman, Russell County
Board of Supervisors
Richlands, VA

The Hon. Janet Howell
VA State Senator
Reston, VA

The Hon. Eugene J. Huang
Secretary of Technology
Richmond, VA

M. Wayne Huggins
Executive Director/Chief Lobbyist
Virginia State Police Association
Richmond, VA

The Hon. Timothy Kaine
Lieutenant Governor
Richmond, VA

The Hon. Judith Williams Jagdmann
Attorney General
Richmond, VA

The Hon. John W. Marshall
Secretary of Public Safety
Richmond, VA

The Hon. Floyd H. Miles, Sr.
Virginia State Delegate
Richmond, VA

The Hon. Brian J. Moran
Virginia State Delegate
Alexandria, VA

Patricia H. Morrissey
Senior National Security Analyst
Science Applications International
Corporation
Potomac Falls, VA

Michael P. Neuhard
Fire Chief, Fairfax County
Fairfax, VA

The Hon. John M. O'Bannon, III
Virginia State Delegate
Richmond, VA

John S. Quilty
Retired Senior Vice President and
Director of the Command, Control,
Communications and Intelligence (C31)
Federally Funded Research and
Development Center, the_MITRE
Corporation
Oakton, VA

The Hon. Beverly J. Sherwood
Virginia State Delegate
Winchester, VA

Suzanne E. Spaulding
Managing Director
The Harbour Group
McLean, VA

Col. Henry W. Stanley, Jr.
Chief of Police, Henrico County
Richmond, VA

Dr. Charles W. Steger
President, Virginia Tech
Blacksburg, VA

The Hon. Kenneth Stolle
Virginia State Senator
Virginia Beach, VA

Regina V. K. Williams
City Manager, Norfolk
Norfolk, VA

Robert W. Woltz, Jr.
President/CEO
Verizon
Richmond, VA

The Hon. Jane H. Woods
Secretary of Health & Human Resources
Richmond, VA

Appendix C-Commonwealth Preparedness Working Group Members

George Foresman, Ex-Officio
Assistant to the Governor For
Commonwealth Preparedness

John Marshall, Ex-Officio
Secretary of Public Safety

Bob Newman, Co-Coordinator
Deputy Assistant to the Governor For
Commonwealth Preparedness

Major Mike Bise
Department of Game & Inland Fisheries

LTC Terry A. Bowes
Director, Bureau of Criminal
Investigations
Virginia State Police

Brett Burdick
Director, Technological Hazards Division
Department of Emergency Management

Dr. Donald Butts
State Veterinarian
Department of Agriculture and Consumer
Services

Janet Clements
Deputy State Coordinator
Department of Emergency Management

Michael M. Cline
State Coordinator
Department of Emergency Management

Colonel Mike Coleman
Department of Military Affairs

Leonard Cooke
Director
Department of Criminal Justice Services

Jeff Deason
Director of Security Services
Virginia Information Technologies
Agency

Marla Graff Decker
Deputy Attorney General
Public Safety & Enforcement Divisio**n**
Office of the Attorney General

Chris Essid
Commonwealth Interoperability
Coordinator
Office of the Secretary of Public Safety

Col. W. Steven Flaherty
Superintendent
Virginia State Police

Julian Gilman
Office of Domestic Preparedness Grants
Administrator
Department of Emergency Management

Buddy Hyde
Executive Director
Department of Fire Programs

Major Michael A. Jones
Assistant Chief of Police
Virginia Capitol Police

Dr. Lisa G. Kaplowitz
Deputy Commissioner for Emergency
Preparedness and Response
Department of Health

Paul E. Lubic, Jr.
Associate Director for Policy, Practice and
Architecture
Virginia Information Technologies Agency

Colonel George Mason
Chief of Police
Capitol Police

Robert Mauskapf
Statewide Planning Coordinator
Department of Health

Constance McGeorge
Special Assistant
Office of Commonwealth Preparedness

John Miller
Chief, Resource Protection
Department of Forestry

Steve Mondul
State Director, Security and Emergency Mgmt.
Department of Transportation

Michael Murphy
Director, Division of Environmental Enhancement
Department of Environmental Quality

Janet Queisser
Emergency Planning and Response Coordinator
Department of Environmental Quality

Charlie Sledd
Program Development Director
Department of Game and Inland Fisheries

Fred Vincent
Commonwealth Security Coordinator
Department of Emergency Management

Tom Wilcox
Department of Game & Inland Fisheries

Appendix D- Governor's Office of Commonwealth Preparedness and Executive Staff

The Office of Commonwealth Preparedness was first created by Governor Warner's Executive Order 07 (02), continued by Executive Order 69 (04), and is responsible for translating vision into reality by synchronizing actions, both public and private, and by insuring that financial resources are being expended on shared statewide preparedness goals. The Office's role is one of policy, coordination, leadership and resource allocation between agencies of state government entrusted with public safety and security responsibilities. The Office serves as a direct liaison between the Governor and Virginia's local governments and first responders on issues of emergency preparedness. It helps educate the public on homeland security issues and responds to inquiries for support and guidance. The Office of Commonwealth Preparedness is the single point of contact in Virginia with the Department of Homeland Security. The Office is leading the effort to secure additional federal funding for preparedness initiatives, as Virginia's unique geographic location - home to the world's largest navel base, a hub for Internet traffic, neighbor to the nation's capitol and backup location for federal operations – places the Commonwealth high on the list of potential terrorist targets.

The Assistant to the Governor for Commonwealth Preparedness serves in a cabinet level position and heads the Office of Commonwealth Preparedness. This new office was established by Governor Warner by Executive Order 07 (02) to lead Virginia's preparedness effort and to coordinate Virginia's security in the fight against terrorism and was continued by Executive Order 69 (04). The Office is charged with the responsibility to work with Virginia's congressional delegation and the President's administration in obtaining additional federal resources for security.

George W. Foresman
Assistant to the Governor for Commonwealth Preparedness

> George W. Foresman serves Virginia's citizens and Governor Mark R. Warner as Assistant to the Governor for Commonwealth Preparedness. In this capacity he is the principal advisor and overall coordinator for homeland security, preparedness, and relations with military commands and installations throughout Virginia.
>
> Foresman chairs the Secure Commonwealth Panel and leads the Governor's related initiative responsible for strengthening Virginia's security and preparedness for emergencies and disasters of all kinds, including terrorism. He serves as Virginia's principal liaison with the White House, Congress, U.S. Department of Homeland Security, and other federal entities to coordinate homeland security policy and programs as well as obtaining resources.
>
> Maintaining a productive relationship with the Department of Defense and Armed Services remains a priority for Governor Warner. Foresman serves as the Governor's direct Cabinet level liaison with top defense and military officials, commands and installations. He is the vice-chair of the Virginia Military

Advisory Council which serves to foster civil-military communication and pro-military policies across Virginia. Foresman also provides oversight of the Commonwealth's activities relative to federal base realignment and closure process.

Foresman is a nationally recognized expert on emergency preparedness and homeland security. He was a member and vice-chair of the Advisory Panel to Assess Domestic Response Capabilities Involving Terrorism, established by Congress in 1998 to evaluate America's readiness for terrorism. The Panel delivered five annual reports to the Congress and President before completing its work in December 2003. More than 125 of the Panel's 144 recommendations have been adopted in part or whole. He frequently is solicited for consultation on national policy issues.

A native of Lexington, Virginia, Foresman joined state government in 1985. He possesses more than 20 years of experience in emergency management, law enforcement, fire and emergency medical service organizations ranging from operations to executive level leadership.

Mr. Foresman is a graduate of the Virginia Military Institute as well as the Virginia Executive Institute.

Robert B. Newman, Jr.
Deputy Assistant to the Governor for Commonwealth Preparedness

Governor Mark Warner appointed Mr. Newman on July 1, 2004. A Brigadier General in the Air National Guard, he is the Vice Director for Operations, Logistics, and Engineering at the United States Joint Forces Command in Norfolk. Following the attacks of September 11, 2001 he was called to active duty and served at the National Guard Bureau in Washington DC. He headed the Domestic Operations Division that was responsible for the development of a critical infrastructure protection program for the fifty-four states and territories.

Newman has been associated with the financial services industry since 1981. He was worked for national and regional brokerage firms specializing in institutional fixed income sales.

Newman is a graduate of the Virginia Military Institute, where he received a Bachelor of Arts degree in Economics, and of Webster University, where he received a Master of Arts degree in Management and Public Administration.

Appendix E-Secure Commonwealth Initiative Working Groups

Virginia Military Advisory Council

The Virginia Military Advisory Council plays a parallel role to the Panel with the active duty military bases located in Virginia, which are vital to America's security defenses and of great importance to the economy of the Commonwealth. The role of the Council is to foster coordination, communication and cooperation between the Commonwealth and the leadership of the U.S. Armed Forces stationed in the Commonwealth. The Council is charged with encouraging regular communication regarding continued military facility viability; the exploration of privatization opportunities; and issues affecting preparedness, public safety and security. Section 2.2-2666.1 of the Code of Virginia established the Council, which is composed of 25 members.

Commonwealth Preparedness Working Group

The Commonwealth Preparedness Working Group is composed of key representatives of state agencies involved in preparedness and homeland security related operations. Members of the Working Group function as a team to support the Panel and coordinate state agency action during threat situations, incidents or challenges facing Virginia. They also propose projects for funding and work hard to break down the old "stovepipe" structure of government. The team meets regularly to coordinate and assess the state's preparedness and readiness. The Working Group is comprised of representatives from the Secretary of Public Safety, Office of Commonwealth Preparedness, Virginia State Police, Department of Emergency Management, Department of Agriculture and Consumer Services, Department of Military Affairs, Department of Fire Programs, Department of Health, Department of Transportation, Capitol Police and Secretary of Commerce and Trade.

Appendix F-Virginia Citizen Corps

Virginia Citizen Corps Program provides an opportunity for citizens of the Commonwealth to take an active role in the provision of security and preparedness in their communities. Local Citizen Corps Councils in every region of the state bring emergency management experts to the table with citizen volunteers to work together to make communities more prepared and secure for emergencies, hazards, threats and disasters of all kinds.

Forty-eight local and six regional Citizen Corps Councils serve the Commonwealth. The Councils coordinate outreach and preparedness programs for 75% of Virginia's population, providing community based training and volunteer activities that assist and support the first responder and public safety communities. Local programs serve more than 70 localities.

Local Citizen Corps programs in Virginia provide outreach, education, training and exercise opportunities to teach citizens of the Commonwealth skills that can be used year-round, in times of emergencies, or during disasters. Citizens learn to conduct damage assessments, provide shelter services, safely operate equipment such as chain saws, support staff in local emergency operation centers, set up and operate amateur radio communication and command centers, make individual and neighborhood preparedness plans, assembly preparedness kits, teach preparedness skills and identify and report criminal and terrorist activities.

Local Citizen Corps Councils provide the oversight for these activities in Virginia. Membership on these local councils must mirror the make-up of the community. Each local council must have representation from first responders, law enforcement, emergency management, local government, health, volunteer community, faith-based community, public utilities, the private sector and citizens.

The five core Citizen Corps programs are Community Emergency Response Team Training (CERT), Fire Corps, Medical Reserve Corps, Neighborhood Watch and Volunteers in Police Service.

More than 3,500 citizens are CERT trained. There are 15 Virginia Medical Reserve Corps programs. There are 4,794 Neighborhood Watch groups in Virginia with an average of 66 households participating in each group. And there are more than 30 local Volunteers in Police Service programs. The Fire Corps is Virginia's newest Citizen Corps program; it is being established under the direction of the Virginia Department of Fire Programs.

Appendix G- Acronyms

BRAC	Base Realignment and Closure
CBRNE	Chemical, Biological, Radiological, Nuclear, Explosives
CCP	Citizen Corps Program
CERT	Community Emergency Response Team
CIPWG	Critical Infrastructure Protection Working Group
COG	Continuity of Government
COOP	Continuity of Operations Plan
DCJS	Department of Criminal Justice Services
DHS	Department of Homeland Security
DOAV	Virginia Department of Aviation
DOD	Department of Defense
EAS	Emergency Alert System
EMAP	Emergency Management Accredited Program
EMS	Emergency Medical Service
EOC	Emergency Operations Center
GIS	Geographic Information System
HSGP	Homeland Security Grant Program
JIC	Joint Information Center
JLARC	Joint Legislative Audit and Review Commission
LETPP	Law Enforcement Terrorism Prevention Program
NCR	National Capitol Region
OCP	Office of Commonwealth Preparedness
OEMS	Office of Emergency Medical Services
ODP	Office of Domestic Preparedness
PIO	Public Information Officer
SHSP	State Homeland Security Program
SIEC	State Interoperability Executive Committee
SWAN	Statewide Alert Network
TSA	Transportation Security Administration
UASI	Urban Area Security Initiative
VBMP	Virginia Base Mapping Program
VCOMB	Virginia Commission on Military Bases
VMAC	Virginia Military Advisory Council
VDACS	Virginia Department of Agriculture and Consumer Services
VDEM	Virginia Department of Emergency Management

VDFP	Virginia Department of Fire Programs
VDH	Virginia Department of Health
VDOE	Virginia Department of Education
VDOT	Virginia Department of Transportation
VEOC	Virginia Emergency Operations Center
VERT	Virginia Emergency Response Team
VGIN	Virginia Geographic Information Network Division
VISWG	Virginia Information Sharing Working Group
VITA	Virginia Information Technologies Agency
VPA	Virginia Port Authority
VR3	Virginia Readiness, Response and Recovery GIS
VSP	Virginia State Police

Appendix H-National and State Guidelines for the Strategic Plan

The Secure Commonwealth Panel adopted this five-year comprehensive all-hazards preparedness strategy to set forth the Commonwealth's vision and priorities for ensuring a secure and prepared Commonwealth.

It is the intent of the Commonwealth to act in alignment with the National Preparedness Goal and seven National Priorities:

1. Implement the National Incident Management System and National Response Plan.
2. Expand Regional Collaboration.
3. Implement the National Infrastructure Protection Plan.
4. Strengthen Information Sharing and Collaboration Capabilities.
5. Strengthen Interoperable Communications Capabilities.
6. Strengthen CBRNE Detection, Response, and Decontamination Capabilities.
7. Strengthen Medical Surge and Mass Prophylaxis Capabilities.

The Secure Commonwealth Initiative's Strategic Plan is also aligned with Virginia's statewide long-term objectives as articulated by the Council on Virginia's Future:

1. Be recognized as the best managed state in the nation.
2. Be a national leader in the preservation and enhancement of our economy.
3. Engage and inform citizens to ensure we serve their interests.
4. Elevate the levels of educational preparedness and attainment of our citizens.
5. Inspire and support Virginians toward healthy lives and strong and resilient families.
6. Protect, conserve, and wisely develop our natural, historical, and cultural resources.
7. Protect the public's safety and security, ensuring a fair and effective system of justice and providing a prepared response to emergencies and disasters of all kinds.
8. Ensure that Virginia has a transportation system that is safe.

Appendix I-Task Force Strategies

Funding Task Force of the Secure Commonwealth Panel

****

Recommendations to The Secure Commonwealth Panel & The Office of the Governor - Commonwealth Preparedness

May 10, 2005

Table Of Contents

Members

The Honorable Katherine K. Hanley, Chair
Former Chairman, Fairfax County Board of Supervisors

The Honorable Frank W. Horton
Former Chairman, Russell County Board of Supervisors

The Honorable Barry Green
Deputy Secretary, Secretary of Public Safety

Regina V.K. Williams
City Manager, Norfolk

Lisa G. Kaplowitz, Ph.D.
Deputy Commissioner for Emergency Preparedness and Response
Virginia Department of Health

James W. Keck
Deputy State Coordinator
Virginia Department of Emergency Management

Philip A. Broadfoot
Police Chief
Danville, VA

R. Steven Best
Fire Chief
Chesapeake, VA

Robert Mathieson
Chief Deputy Director
Department of Criminal Justice Services

Julian Gilman
Virginia Department of Emergency Management

Charles E. Jett
Sherriff
Stafford, VA

James D. Campbell, CAE
Executive Director, Virginia Association of Counties

Malvern R. "Rudy" Butler
1st Vice President, Virginia Association of Counties

Janet Areson
Virginia Municipal League

Ron Carlee
Emergency Services Director and County Manager
Arlington, VA

John C. McGehee
Assistant Administrator
Verona, VA

William R. Nelson, Ph.D.
Public Health Officer/Health Director
Chesterfield, VA

John Crooks
Budget Analyst
Department of Planning and Budget

Pete Sommer
Emergency Management Coordinator
Hampton, VA

Carol Scarton
Purchasing Agent
Prince William, VA

Brent Robertson
Director of Management and Budget
Roanoke County, VA

Suzanne Simmons
Citizen Corps Program Manager
Virginia Department of Emergency Management

Arlene K. Ney
Accountant IV, Finance/Comptroller’s Office
Virginia Beach, VA

Meredith K. Ching
Management and Budget Analyst, Management Services
Virginia Beach, VA

Introduction

The challenge for the Funding Task Force, as reflected in its mission statement, was to find ways to help localities be efficient and effective in funding and implementing appropriate homeland security projects in a timely manner, and to be proactive in responding to possible future federal rules changes.

The Task Force held three teleconferences to discuss issues surrounding current processes and to make recommendations that would improve the process in the future. Because Task Force members represented a wide range of perspectives, a consensus developed that recommendations must include enough flexibility to meet a variety of needs.

Thank you to all the Task Force members, with special thanks to Barry Green and the formula subcommittee.

Kate Hanley, Chair

Mission of the task force

*Examine the methodologies for funding localities and determining what is a reasonable approach for the future, with potential decreases in federal funding likely. Ensure a funding approach that will put taxpayer dollars to the best use for securing all localities in Virginia***.**

Policy Issues

- *Determine how the Commonwealth should approach dispersal of homeland security funding in a way that will increase preparedness and security statewide*
- *Determine how the Commonwealth and its localities can adapt to likely decreases in federal homeland security funding*
- *Develop and evaluate the funding process on both the state and local levels*

Recommendations

I. Policy

Structure and Strategy

The Commonwealth, as a whole, and the individual entities within it need to develop long-term plans for homeland security funding.

Issue 1 - Localities should have long-term homeland security plans and a funding strategy to implement those plans.

Recommendations

1. Each locality should adopt a five-year plan that is compatible with the Secure Commonwealth Panel's strategic plan.

2. The local plans should be updated each year to reflect goals that have been met and new goals/performance measures.

Issue 2 - What should local homeland security funding plans contain and how will they fit into the Commonwealth's strategic plan?

Recommendation

The task force recommends that the Secure Commonwealth Panel, as a whole, address this issue because it is broader than funding.

Issue 3 - If the federal government requires a regional approach to funding homeland security projects, how will the Commonwealth implement that requirement?

Recommendation

Rather than have the Commonwealth define specific regions, localities are encouraged to develop multi-jurisdictional projects. This will allow for different combinations of localities to make proposals addressing a variety of issues.

The Commonwealth's Ability to Adapt to Federal Issues

The Commonwealth should be prepared for possible decreases in federal homeland security funding.

Issue 1 - How can localities best prepare for possible decreases in federal funding?

Recommendation

Each locality spending plan should include proposed items to be purchased (whether goods or services) and should include a prioritization. A prioritized purchase list would better enable localities to identify alternate goods or services to purchase if funding received is less than identified as needed.

II. Process

Efficiency

It is vital that the Commonwealth disperse federal homeland security funds to localities in a clear award letter and in a timely manner. In turn, localities should have a plan for the funds, be prepared to spend them, and report back to the state on how the funds were used to increase their security and preparedness.

Issue 1 - Localities do not know how much federal homeland security money they will receive until after they have passed their budgets.

Recommendations

1. The Commonwealth should publish the Homeland Security grant amounts, as soon as it receives them, so localities can calculate the approximate amount of funding they will receive when calculating their budgets.

2. Local governing bodies have to meet to approve changes to their budgets, which is often necessary regarding homeland security funds as these are dispersed after localities pass their budgets. Thus, there should be a 60-day turnaround between notification of the amount of funding localities will receive and grant proposal submissions. This timeframe will allow local governing bodies in the Commonwealth time to approve changes to their budgets.

3. In order to provide localities with a guaranteed amount of funding for security and preparedness programs, the Commonwealth could appropriate $10,000, in state funding, to localities annually. Federal funding, on a grant basis, would supplement local initiatives.

Issue 2 - Localities are required to spend homeland security funds within a certain time period or the state will re-allocate the unspent money. The funding guidelines and deadlines should be made clear to localities upfront.

Recommendations

1. It is important to continue to deal with localities on a case-by-case basis because each locality is different and will require special assistance or exceptions that the state may provide if it is aware of them.

2. Each locality's funding request should reflect the goals contained in its long-term funding plan.

III. Implementation

Funding Formula

The Commonwealth is charged with dispersing federal homeland security funds to localities. Of the homeland security funds, 80% goes to localities and 20% to state agencies. A clear formula for funding dispersal will allow localities to begin to plan ahead for how much homeland security funding they may receive.

Issue 1 - The funding formula needs to be revamped based on evolving federal criteria, as well as what the Commonwealth has learned from the past funding cycles.

Recommendations

1. Identify the amount of the 80% local share of the total applicable federal grant for the year. This must be done in a timely manner.

2. Each locality (134 in total) will receive a base amount of $10,000, off the top of the 80% share.

3. Of the remaining amount:
   - 35% will be distributed based on population
   - 35% will be distributed based on risk
   - 30% will be awarded through a competitive grant process

4. Competitive grants will be capped at:
   - $100,000 for a single locality
   - $250,000 for a multi-jurisdictional grant including 2-3 localities
   - $350,000 for a multi-jurisdictional grant including 4 or more localities

5. In assessing competitive grant proposals, preference will be given to multi-jurisdictional solutions, and to proposals that

involve promising technology or concepts that may be piloted to determine appropriateness for statewide application.

Issue 2 - What is required of the Commonwealth to implement this new funding plan?

Recommendations

1. The Secure Commonwealth Panel has to complete the statewide strategic plan, and require localities to have plans that comport with the statewide plan

2. The Secure Commonwealth Panel has to decide on risk criteria and how to assign scores to localities based on such criteria

3. The Secure Commonwealth Panel can recommend members/staff, for appointment, to assess competitive grant proposals

Conclusion

In the process of making its recommendations, the Task Force found several issues that are beyond the scope of the funding process and therefore are more appropriately addressed by the Panel as a whole.

The Funding Task Force recommends that each locality have a long-term (possibly 5 years) homeland security plan that identifies projects to be undertaken, and that fits in with the state strategic plan. What those plans should include and how they are developed and reviewed is a broader matter than funding, and should be considered by the entire Panel.

The Task Force recommends that risk should be a factor in evaluating grant applications. Therefore, criteria for determining and evaluating risk need to be established; again, a task beyond the charge to the Task Force.

In conclusion, the Task Force found that a funding process that is transparent at the beginning of a funding cycle, that includes multi-year plans, and that is flexible enough to recognize the diversity of need in the Commonwealth, will be more efficient and effective both for the state and its localities, thereby improving the safety and security of Virginia's citizens.

Intelligence and Information Sharing Task Force

****

Recommendations to The Secure Commonwealth Panel & The Office of Commonwealth Preparedness

May 10, 2005

Table Of Contents

Members

Suzanne E. Spaulding, Chair
Managing Director, The Harbour Group LLC

The Honorable John W. Marshall
Secretary of Public Safety

Robert B. Newman, Jr.
Deputy Assistant to the Governor, Office of Commonwealth Preparedness

Dr. Lisa G. Kaplowitz
Deputy Commissioner for Emergency Preparedness and Response,
Virginia Department of Health

Steven M. Mondul
State Director, Security & Emergency Management,
Department of Transportation

Michael M. Cline
State Coordinator, Virginia Department of Emergency Management

Colonel W. Steve Flaherty
Superintendent, Virginia State Police

Michael P. Neuhard
Fire Chief, Fairfax County Fire & Rescue Dept

Colonel Henry W. Stanley, Jr.
Chief of Police, Henrico County Police

Colonel Michael J. Coleman
Director of Plans, Operations & Training, Department of Military Affairs

Patricia H. M. Morrissey
Senior National Security Analyst, Hicks & Associates, Science Applications International Corp (SAIC)

William H. Parrish
Associate Professor, L. Douglas Wilder School of Government and Public Affairs,
Virginia Commonwealth University

John S. Quilty
Retired, Senior Vice President and Director, MITRE Corporation

Introduction

Mission of the task force

Review strategic information sharing among the various levels and agencies of government and address theses issues from a policy and operations standpoint, based upon what is in place and what the Commonwealth should do in the future.

PROCESS

The Task Force began in the same way that an effective intelligence cycle begins, by identifying information requirements for terrorism preparedness and response in the Commonwealth. This was followed by a discussion of how various state and local entities can contribute to efforts to meet the identified information needs. Key to the discussion was recognition that virtually every player is both a collector and a consumer of relevant information. Finally, the Task Force focused most of its effort on identifying specific challenges to meeting the overall goal of enhancing Commonwealth preparedness through more robust and effective information sharing. The Task Force developed recommendations for addressing each challenge or issue identified. In all of these discussions, the Task Force was mindful of the extensive collaborative structures and processes that are already in place and working well throughout the state.

GUIDING PRINCIPLES

The Task Force recognized that the primary mechanism for intelligence/information sharing will be the new Fusion Center. However, it was also understood that information sharing must extend beyond the Center, through virtual sharing structures, training, and protocols at all levels of government and with the private sector, so that a culture of appropriate and effective sharing becomes ingrained.

Using the statutory authorization for the establishment of the Fusion Center as a guide to legislative and executive intent with regard to information sharing, the Task Force recommendations reflect a broad, inter-agency focus rather than the law enforcement focus that often characterizes other state fusion centers and intelligence/information sharing efforts. Having said that, national guidance documents developed for law enforcement information sharing efforts provided useful checklists for the Task Force as it identified issues and developed proposals.

Similarly, the Task Force understood that the goal is to enhance the sharing of all relevant information, not just that typically labeled as "intelligence." There are many different ways to define "intelligence," which can lead to confusion since readers may be unclear which definition applies in any given context. Thus, the Task Force uses the term "information" unless specifically referring to classified information provided by federal intelligence agencies.

Nevertheless, what is typically referred to as the "intelligence cycle" can serve as a useful overall guide for any organization, including state and local governments, attempting to ensure that it has the information necessary to guide decision-making. The process begins with identifying information requirements, followed by an evaluation of how those requirements are being met currently, where there are gaps, and how those gaps can be filled through additional or improved information gathering/collection efforts. The next step is ensuring that the information, once gathered, is disseminated to those who need it. This includes analysts who can put the information in context, as well as ultimate end-users. These "consumers" should then evaluate the information and provide feedback to the requirements process, assessing how well the information meets the needs of the user and what gaps still exist.

The entire process must be guided by clear policy directives, implemented by an appropriate governance structure, informed by protocols and interagency agreements, and inculcated through appropriate training. The need to protect civil liberties and sensitive information, including information implicating privacy concerns, law enforcement sensitive information, information governed by HIPPA and other health and medical requirements, must be fully considered at every level of the process.

Finally, the Task Force recognized that the Commonwealth's information sharing must take into consideration federal initiatives, capabilities, and requirements.

These are the key issues and challenges that informed the Task Force as it formulated the recommendations listed below.

Recommendations

I. Policy

Civil Liberty Protections

Terrorists seek to destroy lives and our way of life. The homeland security imperative is to deny them both of these objectives. Thus, civil liberty protections must be an inherent aspect of the Commonwealth's enhanced information sharing initiatives.

Issue 1 - Who should be in charge of overseeing the protection of civil liberties in the Commonwealth in the context of these intelligence and information sharing initiatives?

Recommendation

Ultimately, the responsibility to preserve civil liberties cuts across all agencies and entities involved and comes together at the level of the chief executive. Thus, the Governor's Office of Commonwealth Preparedness and/or the Governor's policy office should be responsible for ensuring that there is an independent arbiter to safeguard the civil liberties and privacy of the Commonwealth's citizens throughout the information collection, analysis, and dissemination process. Appropriate consideration should be given to including non-governmental representatives as part of this important oversight function.

All Hazards Approach

While the focus of Task Force was terrorism-related information, the long-term goal of the fusion process is to manage all risks to the Commonwealth, not just terrorist threats.

Issue 1 - How can the Commonwealth ensure that the information sharing process can ultimately serve preparedness needs beyond the terrorist threat?

Recommendation

The Office of Commonwealth Preparedness should be tasked with ensuring that local governments and first responders are included in discussions on Commonwealth security and preparedness and in the intelligence and information sharing process, as well as identifying new partners.

II. Governance

It is essential to effective governance of the information sharing process that roles and responsibilities are clearly established. Responsibility for ensuring Commonwealth preparedness with respect to the terrorist threat falls upon the Governor, who has designated the Office of Commonwealth Preparedness as his primary executive agent in this regard. Responsibility for implementation of this authority is spread across many departments, agencies, and offices at the state and local level. The private sector also has some preparedness obligations. In addition, the legislature provides statutory authority and funding for effective implementation of these fusion efforts.

Issue 1 - How does the Commonwealth ensure effective management of this collaborative process?

Recommendations

1. A governance structure that includes broad representation from all appropriate entities at the state and local level, as well as the private sector, should be established for the information sharing process. This structure should report to the Governor, through the Office of Commonwealth Preparedness.

2. As a key element of the information sharing process, the Virginia Fusion Center should, consistent with the authorizing legislation, be operated by Department of State Police in cooperation with the Department of Emergency Management and other state and local agencies and private organizations, pursuant to the guidance and direction of the Governor, on behalf of this collaborative governance structure. The director of the Fusion Center should report directly to the head of this governance structure, as designated by the Governor.[1]

A(v)[1] Section 52-47 of the Code of Virginia was enacted by the General Assembly in 2005 to establish Virginia's Intelligence Fusion Center. That section states: "*The Governor shall establish, organize, equip, staff, and maintain a multiagency intelligence fusion center to receive and integrate terrorist-related intelligence and information. The Department of State Police shall operate the facility, as directed by the Governor and in cooperation with the Department of Emergency Management and other such state and local agencies and private organizations as the Governor may deem appropriate. The fusion center shall collect, analyze, disseminate, and maintain such information to support local, state, and federal law-enforcement agencies, and other governmental agencies and private organizations in preventing, preparing for, responding to, and recovering from any possible or actual terrorist attack.*"

Issue 2 - The legislature must be given the information it needs in order to better understand the requirements associated with requests for resources to enhance both the security and preparedness of the Commonwealth.

Recommendations

1. Members of the General Assembly should be provided with intelligence assessments that will help them fully appreciate potential threats and security issues confronting the Commonwealth. The Intelligence Fusion Center should prepare an annual Intelligence Assessment that is drawn from national intelligence assessments/estimates, Department of Homeland Security and Federal Bureau of Investigation Advisories and Alerts, and other sources of intelligence and information to include "Open Source" reporting, as well as local and state information and intelligence that can help to particularize the federal intelligence to Virginia. The Intelligence Assessment should be prepared up to the sensitive but Unclassified Level. The Assistant to the Governor for Commonwealth Preparedness will coordinate annual review and approval of the Commonwealth's Annual Intelligence Assessment with the Secretary of Public Safety, Adjutant General, Superintendent of Virginia State Police, Coordinator of Emergency Management, Commissioner of Health, and others as needed, prior to release. Upon approval of the Intelligence Assessment, the Director of the Intelligence Fusion Center should brief designated members of the Governor's Cabinet, key leadership within the Commonwealth's General Assembly to include designated Committee Chairs and the Speaker of the House. This briefing should be provided within the first three days of the General Assembly's Annual Session.

2. Additionally, the Intelligence Fusion Center should prepare Sensitive But Unclassified Quarterly Intelligence Summaries that will be made available to designated Cabinet level officials and designated members of the General Assembly.

III. Structure and Strategy

There is an evident need to share information horizontally across agencies and departments, vertically between the levels of government, and between the government and the private sector. The Fusion Center will provide the primary structure for the information sharing process.

Issue 1 - How can the Commonwealth best ensure that the Fusion Center succeeds in improving information flow between agencies and maximize their input in the fusion process?

Recommendations

1. At the state level, the Fusion Center concept should be designed to facilitate effective information sharing by ensuring that individuals representing the key players can come together in a common facility and providing the nexus for an ongoing intelligence exchange. While this may not eliminate all stove piping and cannot force sharing at the federal and local levels, it does provide a mechanism for fusing information at the state level and may have some impact on forging a new culture beyond. Thus, the Fusion Center will be an ongoing effort to facilitate sharing of information and intelligence.

2. When the Fusion Center is operational, each agency should have identified a representative for the Center. This individual will obtain relevant mission-critical information as it comes into the Fusion Center and will be the point of contact for his/her agency in the Fusion Center. Agency representatives will be responsible for receiving and sharing information in the Fusion Center. Because each agency will have a designated representative for the Fusion Center, the VISWIG will no longer be necessary and will be dissolved a year after it opens.

Issue 2 - How can the Commonwealth ensure local input in the fusion process both in generating information and analyzing information and intelligence coming into the Fusion Center?

Recommendations

1. Localities should have the opportunity to have a designated representative for the Fusion Center, who will be responsible for receiving and sharing information.

2. Local Chief Administrative Officers should designate two law enforcement and two non-law enforcement representatives for the Fusion Center. The local representatives will be responsible for receiving and sharing information.

3. Localities should be encouraged to share information that may be relevant with the Fusion Center as well as the Joint Terrorism Task Force (JTTF).

IV. Working within the federal context

The Commonwealth must be prepared and willing to work with the federal government to establish an information sharing environment. The federal government is creating an information sharing environment, through the National Intelligence Reform Act, the states must do so as well. This will require working with the federal government on the handling of federally-classified and sensitive information, as well as representation by and at the federal level.

Issue 1 - How can the Commonwealth best manage the information flow between the Commonwealth and the various federal entities?

Recommendations

1. The Office of Commonwealth Preparedness should work with the federal government to establish appropriate mechanisms for obtaining information/data from as many different sources as possible for the fusion process.

2. Within the DHS umbrella, Homeland Security Operations Center (HSOC) is likely to remain the primary source of information for the Fusion Center. Therefore, the Commonwealth should consider undertaking efforts to maintain a representative at the HSOC. Regular reporting to DHS/HSOC will affect local funding streams.

3. The National Guard, reporting for the Defense Department, should have full-time representation in the Fusion Center, giving the state a direct link to the military. This person will be trained in accordance with the fusion process requirements.

4. The FBI, on behalf of the Justice Department, should place an analyst within the Fusion Center, which will greatly enhance the exchange of mission critical information.

5. Information sharing mechanisms within the Fusion Center should also incorporate the Centers for Disease Control, which can report on behalf of the Department of Health and Human Services.

V. Implementing Effective Information Sharing

Effective information sharing at all levels of government and with the private sector will require attention at each step in the information cycle, starting with efforts to ensure that all appropriate players are contributing to meeting identified information needs, handling the information appropriately, effectively analyzing that information, and disseminating the information to all those who need it. The consumers of this information must then have a mechanism for updating information requirements as needed.

Getting information into the fusion process

Issue 1 - Policies and procedures must be developed to ensure that information flows into the fusion process in an appropriate way and from as many sources as possible at all levels.

Recommendations

1. Descriptions of how information flows into the fusion process should be included in the Standard Operating Procedures for the Fusion Center, to include:

   - **Who** may submit with complete contact data
   - Submission Protocol **(How and When)**
   - Types of information to be submitted (**What**)
   - Consolidation of information at the local level
   - Evidentiary chain-of-custody protocol for physical input (e.g. suspicious substances)

2. All personnel along the information chain should be vetted (background checks, even if they will not require clearances) and receive training.

3. State and local officials should work together to facilitate the gathering and sharing of information/intelligence so that leads and information/intelligence can be further developed. Once this occurs, information will be generated and investigated at the state and local levels, and not solely at the federal level.

4. Procedures should be developed to minimize duplication of investigative efforts.

Analyzing information

For the fusion process to be successful, input is required from all agencies, levels of government, and the private sector. Only then will the Center analysts be able to connect the dots in all areas to evaluate all hazards to the Commonwealth.

Issue 1 - Analysts in the Fusion Center must understand local/regional issues and have local/regional connections.

Recommendations

1. While it may not be feasible to match Fusion Center analysts to geographical areas in the state, the Center should strive for collective expertise in areas with varying types of concerns and conditions (urban & rural, industrial & agricultural, inland & coastal, etc.).

2. Temporary exchange of personnel with federal and local intelligence centers or short tours of duty in the Fusion Center for local personnel should be considered to expand understanding of varying viewpoints, develop partnerships, encourage cross-pollination, and establish lines of communication.

Issue 2 - The Commonwealth must ensure that the knowledge and expertise of the responder community is brought to bear in analyzing information through the fusion process.

Recommendations

1. The Fusion Center should include fire service and EMS through representation from Department of Fire Programs, agriculture, and Office of Emergency Medical Services of the Health Department in the expanded analyst cadre at the Fusion Center.

2. The Center should maintain regular contact with function-specific analysts from other agencies and the private sector (health & medical, agricultural, transportation, fire services, environmental, military, industry & infrastructure, etc.) and bring them into the fusion process when needed.

3. Secure communication mechanisms should also be established to facilitate contacts in risk- and threat-specific arenas (ports, large event managers, high hazard industry, etc.). Outreach and education programs should be developed to encourage and insure these contacts.

Issue 3 - There should be specific qualifications for the Fusion Center's intelligence analysts.

Recommendations

1. Fusion center analysts should collectively have local/regional, preferably Virginia, government and emergency responder background as well as expertise in the field of intelligence analysis.

2. Virginia should develop a training and education program on intelligence/information sharing:

   - Base level "of what to look for" for wide range front-line workers
   - Mid-level training for localities/agencies in "basic analysis"
   - Higher level training for local and state officials in "detailed analysis and trend recognition.

Handling sensitive information

There are potentially many categories of sensitive information that agencies and entities will be providing to the fusion process, including classified information, law enforcement sensitive information, information raising privacy issues, sensitive health information, and even proprietary information. There must be clear policies and protocols governing the handling and dissemination of this information, with state-wide application.

Issue 1 - State agencies need a system and protocols for managing and protecting sensitive information, including classified information/intelligence.

Recommendations

1. Virginia State Police (VSP) is developing a set of guidelines for the Fusion Center; however, *an executive order is needed* to extend these guidelines beyond the Center and beyond law enforcement/intelligence information. The Attorney General should be consulted on these guidelines and any executive order in order to ensure full compliance with legal requirements, particularly as relates to privacy and civil liberties concerns.

2. Virginia Department of Transportation (VDOT) also has a classification process; this could possibly be expanded statewide.

Issue 2 - What requirements should be in place regarding the individuals who participate in the fusion process but do not hold a federal security clearance?

Recommendation

State agencies and members of the private sector are not required to acquire a federal secret clearance. State agency and private sector personnel will undergo a State Police background investigation that will allow access to the high-security area of the Fusion Center.

Issue 3 - Which entity will be responsible for disseminating classified information to various agencies, etc.?

Recommendation

The Information Classification Unit (ICU) should forward information to state agencies and the private sector on the basis of a mission-related authorization- and need-to-know. This will enable the state to share information with people throughout the state who do not hold a federal security clearance.

Issue 4 - The state should continue to work for federal security clearances for as many state personnel as possible.

Recommendations

1. The Office of Commonwealth Preparedness will submit a clearance recommendation list, of 30 state personnel, to the Department of Homeland Security.

2. In addition, because the overall lack of clearances for state employees outside of the Fusion Center is not likely to change, protocols should be developed for properly “scrubbing” information so it can be disseminated outside of the intelligence community. These protocols need to be agreed upon between the levels of government and agencies and should be implemented nationwide.

Issue 5 - Aside from legal restrictions, agencies are often reluctant to share information because they fear that another agency may prematurely act on shared information without coordinating the action, thus possibly jeopardizing ongoing efforts or initiatives.

Recommendations

1. When the Fusion Center disseminates information, the lead-Action agency should be noted for reference and as a point of contact for follow-up questions.

2. Federal information/intelligence of a classified nature (under the National Security Act) has clear penalties for improper disclosure. Once the Commonwealth is capable of implementing its own state-specific classification system, legislation should be considered to provide penalties for its inappropriate release.

Evaluation and Feedback

It is important throughout the fusion process to keep in mind the ultimate goal is not just information sharing, but providing decision makers at all levels with the information that they need to better understand the threat, vulnerabilities, and ways to manage the risk of a terrorist attack. It is with this objective in mind that consumers of the information, from analysts to first responders, legislators, executive officials, and the Governor, should have a process for providing feedback on the quality of the information and updating information needs. In the world of intelligence, this is often called a "requirements process."

Issue 1 - How can the Commonwealth best ensure that the fusion process is dynamic, so that it can continually improve and respond to evolving information needs?

Recommendation

A formal requirements process should be established, managed by the Fusion Center, in which all relevant entities would have an opportunity to indicate their information needs and evaluate information provided through the fusion process. Each entity should designate an official who will be responsible for ensuring that the entity participates effectively in the requirements process. The Fusion Center should designate an official to manage the process and ensure that requirements are passed on to all entities that are in a position to gather information to meet those requirements.

Mass Fatalities Management Task Force of the Secure Commonwealth Panel

****

Recommendations to The Secure Commonwealth Panel & The Office of the Governor - Commonwealth Preparedness

July 13, 2005

Table Of Contents

Members

The Honorable Jane Woods, Chair
Secretary of Health and Human Resources

William C. Armistead
Disaster Preparedness and Response Director
Office of Planning and Development, Virginia Department of Mental Health, Mental Retardation, & Substance Abuse Services

Michael Berg
Regulatory and Compliance Manager
Virginia Department of Health

Brett Burdick
Director, Technological Hazards Division
Virginia Department of Emergency Management

Michael M. Cline
State Coordinator
Virginia Department of Emergency Management

Colonel Michael Coleman
Deputy Chief of Staff Operations
Virginia National Guard

Marla Decker, J.D.
Deputy Attorney General
Public Safety & Enforcement Division
Office of the Attorney General

Paul B. Ferrara, Ph.D.
Director
Department of Forensic Science

Marcella Fierro, M.D.
Chief Medical Examiner
Virginia Department of Health

Lori Hardin
Statewide Mortality Planner
Office of the Chief Medical Examiner
Virginia Department of Health

Gail D. Jaspen
Chief Deputy Director
Virginia Department of Health Professionals

John W. Jones
Executive Director
Virginia Sheriffs' Association

Lisa G. Kaplowitz, M.D.
Deputy Commissioner for Emergency Preparedness and Response
Virginia Department of Health

Bruce Keeney
Executive Director
Association of Independent Funeral Homes of Virginia

Art Lipscomb
Legislative Director
Virginia Professional Fire Fighters Association

Constance McGeorge
Special Assistant to the Governor
Office of Commonwealth Preparedness

Susan Motley
Executive Director
Virginia Funeral Directors Association

Major Robert B. Northern
Deputy Director, Bureau of Field Operations
Virginia State Police

Bud Oakey
Managing Director and CEO
Advantus Strategies LLC

Mandie Patterson
Victim's Services Section
Department of Criminal Justice Services

Dana Schrad
Executive Director
Virginia Association of Chiefs of Police

Tricia Snead
Manager, Disaster Assistance/Emergency Planning
Virginia Department of Social Services

Robert B. Stroube, M.D., M.P.H.
State Health Commissioner
Virginia Department of Health

Richard E. Trodden
Arlington County’s Commonwealth’s Attorney

Elizabeth Young
Executive Director, Virginia Board of Funeral Homes and Embalmers
Virginia Department of Health Professionals

Introduction

I am pleased to submit to the Secure Commonwealth Panel the report from the Mass Fatality Management Task Force.

The Virginia Secure Commonwealth Panel was tasked overall with assessing the state of the Commonwealth' s preparedness and security in response to the all-hazards terrorist attacks threatening the United States since September 11, 2001. All aspects of the lives and activities of the citizenry have been under review for issues relating to health, safety and security in order to develop recommendations for improving the security of and the official and societal response to a mass fatality event and to enhance the survival of the citizens. The latest round of panel task forces have dealt with intelligence and information sharing, funding, public/private cooperation, and performance measures and has developed recommendations for decision making, changes in statutes and public policy.

The Mass Fatality Management task force was specifically charged "to go beyond operational issues to address decision-making and statutory and public policy issues regarding mass casualty events."

To accomplish this task, public and private parties that interface with the death event met to identify and address issues relating to mass fatalities. A mass fatality event, from an all hazards point of view, would include fatalities due to naturally occurring weather events such as flood or earthquake to terrorist events resulting in thousands of homicide deaths, either all at once, as in attacks on the World Trade Center and Pentagon, or, over time, as would be the natural history of a biologic attack epidemic as exemplified by the Virginia anthrax bioattack.

Chaired by The Honorable Jane Woods, Secretary of Health and Human Resources, the panel brought together agency representatives of the Governor's Office of Commonwealth Preparedness, Departments of Health, Office of the Chief Medical Examiner, Emergency Management, Emergency Medical Services, Virginia State Police, Health Professions, Criminal Justice Services, Mental Health, Office of the Attorney General and Commonwealth's Attorneys and Department of Military Affairs. Private sector collaborators included representatives of Funeral Homes and Embalmers, Virginia Professional firefighters, Virginia Association of Chiefs of Police, and Lobbyists for the funeral service sector.

I believe you will find the background information and recommendations contained herein meet or exceed those requirements and provide the Commonwealth with sound suggestions for measures that will enhance our collective and regional preparedness. I extend my thanks to all the Task force members who gave generously of their expertise and time; but especially we all owe great thanks to Dr. Lisa Kaplowitz, M.D. and Dr. Marcella Fierro, M.D. for their unflagging dedication and commitment to this work.

Mission of the task force

The mission of the Mass Fatalities Management task force is to identify decision-making, statutory and public policy issues the Commonwealth would face in the event of a mass casualty incident and make recommendations to the Secure Commonwealth Panel and the Governor’s Office of Commonwealth Preparedness on how best to address these issues prior to a mass casualty event to better prepare the Commonwealth for an effective and efficient response effort.

Policy Issues

- Determine how to best address outstanding administrative issues the Commonwealth would face following a mass casualty event

- Determine which legal issues the Attorney General’s office should review and how best the Commonwealth might address these issues

- Identify which departments and agencies require funding to train for and respond to a mass casualty event

- Determine what is required to successfully set up and maintain a Family Assistance Center after a mass casualty event

- Determine how best to address issues the Commonwealth would face in a mass casualty event that would require legislation for improvement

Recommendations

I. Administrative Issues

Crisis Response Teams and Volunteers

New policy should be developed regarding how best to staff, train, utilize, and protect the Office of the Chief Medical Examiner (OCME) crisis response team and the volunteers (to include first responders, medical examiners, etc.) who respond to a mass fatality event in Virginia.

Issue 1 - A Disaster Mortuary Response Team or a DMORT is a group of essential personnel who respond to mass fatality events. The federal government supports federal DMORT teams that other states request for assistance. Historically, DMORT teams have been supplied to jurisdictions that had little or no resources for managing an event or have experienced overwhelming casualty events. The September 11 plane crash in Pennsylvania is an example of the former; the World Trade Center is an example of the latter where they continue to recover fragments of victims for identification. Virginia's Medical Examiner System, with the addition of some supplemental resources, could have managed the Pennsylvania event as well as the event at the Pentagon. In any series of multiple coordinated terrorist events federal DMORT teams may not be available to supplement Virginia if they are deployed to jurisdictions with fewer resources. Given Virginia's high risk status, as

Disaster Mortuary Team (DMORT)

Team Management

- **Chief Medical Examiner (1, 1)**
- **Assistant Chief Medical Examiner (1, 11)**
- **Administrative Officer (1, 1)**

Forensic Personnel

- **Pathologist (3, 11)**
- **Odontologist (3, VA dental team))**
- **Dental Assistant (3, as team provides)**
- **Anthropologist (3, 2)**
- **Fingerprint specialist (3, DFS will supply)**

Disaster Scene Personnel

- **Search/recovery personnel (12,4 OCME) Inv. & V**
- **Cadaver dog handlers (3,0) *will request Fairfax team**
- **Surveyors/gridders (3,0) Inv.**
- **Body recovery (5,0) Inv. & V**
- **Underwater recovery (4,0)**

Morgue Personnel

- **Body tracker (16, 0)**
- **Mortuary Officer (6,4) Inv.**
- **X-ray technician (3, 0)**
- **Photographer/videographer (12, 0)**
- **Medical records technician (6,6)**
- **Supply officer (4,0)**

Family Assistance Center

- **Mortuary officer 10, 0**
- **FAC manager**
- **Interpreters (3, 0)**
- **Support Personnel**
  - **Mental Health/CISD Specialist (1,0)**
  - **Communications manager (3,1)**
  - **Safety Officer (1, 0)**
  - **Equipment operator (1,0)**
  - **Team Physician/PA/Nurse (1,0)**
  - **Security officer (3,0)**

evidenced by the Pentagon and anthrax attacks, Virginia needs to supplement the core elements of a Virginia OCME DMORT team that are already in place within the Medical Examiner System.

A DMORT team usually consists of a certain number of team management personnel, forensic personnel, disaster scene personnel, morgue personnel, and staff to operate and manage the family assistance center. However, the Commonwealth is lacking personnel to support various positions on the DMORT team.

The sidebar contains a list of essential personnel for a DMORT. The first number indicates the "normal" number of positions on a team; the second number indicates the OMCE capabilities to fill the position with current staff. "V" indicates a plan to fill with volunteers. "Inv" indicates an investigator position needing to be filled to accomplish the task.

Recommendation

Establish 12 full-time equivalents and funding for medical investigators to give the Commonwealth more personnel who can provide staff support in a mass casualty event.

Issue 2 - How can the state best utilize volunteers in a crisis event given tasks, confidentiality, evidentiary issues and liability?

Recommendations

1. The OCME, working with the Virginia Funeral Directors Association (VFDA) - which will serve as the lead funeral group), the Association of Independent Funeral Homes of Virginia (IFHV), and the Virginia Morticians Association (VMA) will identify funeral service licensees who are willing to be volunteers and will ask for Emergency Preparedness and Response funding, through the Virginia Department of Health (VDH), for criminal background checks.

2. The Virginia State Police (VSP) will complete initial volunteer background checks during volunteer training. Additional background checks will be completed, as necessary, for those who are utilized in a crisis event.

3. OCME will obtain the list of people (funeral service licensees and physicians), who are willing to volunteer in a mass casualty event, from the Department of Health Professionals to proceed with training and initial background checks.

Issue 3 - The Medical Examiner must ensure the safety of those handling contaminated remains and the safety of the public.

Recommendations

1. Consider amending the Code of Virginia to provide the Health Commissioner with the authority to make the call on the safety of the return of human remains after a chemical or biological attack. This decision should be made in conjunction with political and health officials.

2. Explore a Bio-Watch program – which is an early warning system to detect biological agents through continuous air sampling throughout OCME Morgues and multiple indoor detection sensors in the coolers and over the autopsy tables.

3. The VDH should work to implement precautions, to protect the staff of Funeral Directors, as developed by the National Funeral Directors Association.

Issue 4 - How many staff can/will actually report to a mass casualty event?

Recommendation

OCME will survey its staff for availability to volunteer in a crisis event and repeat periodically and will add ability to respond to position descriptions.

Issue 5 - Following a mass casualty event the OCME and the lead law enforcement agency should be called upon to evaluate the situation and make determinations on the appropriate specialized skills needed. Historically, through drills and exercises, other agencies that are not subject matter experts (Forensic Scientists) have called DMORT without first consulting OCME. Despite many of the same “lessons learned” statements following drills, OCME continues to be left out of drills and exercises and anticipates the same will occur again.

Recommendation

The OCME and Virginia Department of Emergency Management (VDEM) are the organizations that will need to identify the personnel assets medical examiners will need for body management for the Governor to request in accordance with standard procedures.

Issue 6 - The OCME has not been eligible for grant funds (as it is a statewide organization, not local) to train the funeral service licensees and other forensic specialists in mass fatality event response.

Recommendation

It is anticipated that VDH will take a lead role in providing training to potential volunteers in advance of actual need; however, OCME requires funds to train its volunteer specialists.

Jurisdiction

It is vital that the various levels of government and agencies that will respond to a mass casualty event understand who has jurisdiction and/or will take the lead during the response and recovery efforts following the event.

Issue 1 - Jurisdictional issues on the management of the deceased are too vague and unclear in the National Response Plan.

Recommendation

The Virginia Department of Emergency Management (VDEM) and the Office of the Attorney General (OAG) will try to develop a Memorandum of Understanding (MOU) with federal authorities that clarifies jurisdiction in a mass casualty event that occurs in the Commonwealth. VDEM will take the lead to initiate these discussions by 9/1/05. Discussions will include: OCME, VSP and VDH from the state and the Department of Homeland Security will determine which federal entities should attend.

Issue 2 - Public Safety and Health entities need to recognize and consider "conflicts" prior to an event of this magnitude to prevent the rise of jurisdictional issues during and after a crisis event. This will enable these entities to work together to plan for and respond to a crisis more efficiently and effectively.

Recommendation

Policy planners for Public Safety, VDH and OCME want to develop MOUs and meet once a year to refine these agreements. The Federal Bureau of Investigation (FBI), VSP and local law enforcement, Medical Examiners, the Virginia Department of Social Services, and the Department of Mental Health, Mental Retardation and Substance Abuse Services (DMHMRSAS) should all be included in these agreements. The OCME and the State Health Commissioner will initiate contacting someone at the federal level to get this recommendation moving.

Issue 3 - The OCME should be the only agency (in conjunction with the local community leadership) that is authorized to approve the establishment of morgues in mass fatality events under the jurisdiction of the OCME. In both the 9-11 Event at World Trade Center and Determined Promise 2004 (DP04) exercise in Virginia, non-medical examiner organizations identified and opened morgues without the knowledge of the OCME. In New York, so many agencies opened morgues without the OCME and Police Department's knowledge, it was unmanageable. Some unauthorized morgues had policies to strip all remains and store the physical evidence in lock boxes, which severely hampered victim's identification (physical evidence should only be removed in the morgue after documentation). Other morgues were allowing any person to enter and view the remains, even if the persons were not next-of-kin. In DP04, the Central Regional Department of Health selected the two largest food distribution warehouses in central Virginia, which would have resulted in the Commonwealth purchasing and compensating two retail corporations for their losses.

<u>Recommendation</u>

The OCME should be the final approval authority for any morgue, and its management, established in Virginia (if the OCME is the jurisdictional authority for the event). This will better enable the state to coordinate and manage the storage and handling of physical evidence as well as human remains. Access to morgues is an OCME procedure

Communication

The various state health agencies need a reliable communication system to enable them to coordinate the response and recovery efforts after a crisis event.

Issue 1 - Include the OCME in any communications plans to be developed by the VDH. Currently, 45% of deaths in Virginia occur in hospitals and a better communication system will enable hospitals to interface with OCME to report any suspicious deaths in a timely manner.

<u>Recommendations</u>

1. VDH should include the OCME in any communications plan that connects the VDH with hospitals.

2. Programmable radios should be available to the OCME in a multiple fatality event. Brett Burdick, at VDEM, will be the lead on this project to determine how many radios are required and what functions they should include.

3. VDH will work with OCME to coordinate a better communication system with regional hospitals.

Issue 2 - Need to reform National Incident Management System (NIMS) to include medical examiners and coroners in the communication/decision process. NIMS/Incident Command System (ICS) does not properly address the functional tasks of the medical examiner in the response protocols. The ICS stops at the point where patients die in triage and a "Morgue Manager" is assigned to protect the remains. ICS does not address the incorporation of the medical examiner into the system, therefore first responders think once the Morgue Manager is established the issues go away.

Recommendations

1. Include the OCME in the unified command with the operational law enforcement investigative agencies to develop appropriate incident action plans.

2. Other agencies may also have to be included in the unified command structure, as appropriate to include those managing the Family Assistance Center, those mitigating the contaminates on the remains, etc.

3. Fire Programs will lead training and incorporate new plans into this system.

Issue 3 - The National Response Plan does not address mortuary affairs appropriately. There is no reference to law enforcement's role in death investigation, forensic examinations, family assistance, personal effects management, criminal investigations, or death notifications to families, as well as release and dispositional matters.

Recommendation

Virginia VDH personnel are on working groups, which have been permitted to interface with the Department of Homeland Security (DHS) and the National Incident Management System integration center to provide feedback on the newly developed plans for the federal response. This task force recommends that these groups include the OCME's State Medical Examiner to provide input into these plans and be part of the working groups for the DHS/state revisions to the National Response Plan.

Fatality Management

It is essential to determine how best to identify, transport, and dispose of human remains in a mass fatality event, as well as how to protect the personnel handling the remains.

Issue 1 - The state needs to determine if the identification process in highly fragmented cases will include the testing of ALL tissue or just a sufficient amount of tissue will be processed until all the victims have been identified (the remainder will be considered “common tissue”). Does the state identify all of the victims or all of the pieces of human remains?

Recommendation

If the event is a closed event, meaning all of the victims are known and subsequently identified, identification of human remains will cease and a respectful final disposition made of the “common tissue”. If the event is open, meaning all of the victims are not known, the state will work to identify all of the “common tissue”.

Issue 2 - Will the state have access to Dover? Virginia was denied access in the Determined Promise 2004 drill despite legislation that states Virginia is allowed access to Dover Air Force Base Port Mortuary in a mass fatality event.[2]

Recommendation

Negotiations are currently under way between the Commonwealth and the Federal Secretary of Health and Human Services to ensure the state will have access to this mortuary should a mass fatality event occur.

Issue 3 - The state needs a policy on how to transport contaminated remains within the state and across state and/or international borders.

Recommendation

Transportation services are available under the funeral licensee laws, from licensed funeral service establishments and from registered surface transportation removal services. The state should determine if there is a federal regulation for transportation of human remains and work out an MOU if possible, otherwise the state should proceed to move remains as needed.

A(vii)[2] Joint Publication 4-06, in both the current 1996 version and the current version (under revision) state: “The use of the Dover Air Force Base Port Mortuary is an option available to civilian authorities.” There are no caveats in the publication on distance of authority, state, city, county authorities, etc.

Reporting - Format and Structure

Following a mass fatality event, it is vital that the response teams are able to adequately document action taken. Reporting is a vital tool that, if streamlined and structured, will better enable decision-makers to determine what next steps need to be taken for the safety of the Commonwealth as well as limit confusion during and after event response.

Issue 1 - There are no common forms or format for Emergency Operations Center needs requests. Each request is reformatted and reinterpreted. There should be national standards to address this issue. In drills where the OCME has been able to submit requests for additional services, the request was re-written and mis-interpreted by Emergency Support Functions (ESF 8) staff in the Virginia Department of Health Emergency Contact Center (ECC??) / state Emergency Operation Center (EOC) or in the local EOC. If the OCME were permitted to submit its own requests for the required services and if each agency utilized the same form, while cross-referencing the tracking numbers on the form, the original intent of the request would be maintained and the required resources would be obtained.

<u>Recommendations</u>

1. A uniform request form/format should be developed that be utilized by local, state, and federal agencies.

2. Web EOC (Emergency Operation Center) is a system under development that will create a single form for everyone to use. VDH and VDEM are leading this initiative. It should be completed by the end of the year.

Issue 2 - The state has a fragmented reporting structure with no real time direct contemporaneous reporting 24/7. Reports on medical examiner cases, other than homicides, suicides and deaths suspicious for violence, are often delayed with receipt of reports from local medical examiners at district offices measured in days to weeks to months. These delays inhibit the capture of deaths due to infection that could be a bioterrorism or emerging infection death, which could appear natural.

<u>Recommendations</u>

1. The OCME needs all deaths reported directly in real time 24/7 by local medical examiners and investigators to a district office, where in-house trained medical investigators can advise on jurisdiction, screen for bioterrorism and emerging infections, and make the real-time determination of management. (This could serve both local medical examiners

and localities lacking a local medical examiner. It should also capture bioterrorism deaths out of hospitals, masquerading as natural deaths).

2. Virginia should provide 12 full-time equivalents for medical investigators and funding to enable 24/7 direct reporting to district offices of all death reports contemporaneously. The usual reporters are medical examiners, law enforcement, hospitals, and EMS. These additional staff and funds would allow for screening for bioterrorism and infectious death and reporting in real-time for determination of jurisdiction and management.

3. To assist first responders with reporting, pocket cards with Med-X signs/symptoms and OCME contact information were distributed. (This will alert first responders when a report should be made to the local medical examiner and provides them with the necessary contact information so the report can be made in a timely manner.) *OCME is working to develop a CD of these pocket cards to give to organizations that can then disseminate the information. This effort to educate more first responders across the state is an inexpensive and efficient approach.

Public Relations

A key aspect of dealing with a mass fatality event is the success of communicating with the public in terms of what the citizens can expect from government and medical officials as well as how the family members can best assist the response teams in identifying lost loved ones.

Issue 1 - The state will need a committed VDH public relations person to coordinate dealing with the media/families on fatality management issues.

Recommendation

VDH has secured Jeffrey Caldwell as the official Public Information Officer (PIO) for the OCME. He will receive training in the current public relations crisis plan along with the four regional PIOs and any other PIOs who have not yet received training in this area.

Issue 2 - The Commonwealth needs to develop policy standards that are acceptable to the public with regard to expectations of identification of human remains.

Recommendation

Virginia must develop standards within *each* event as to what is reasonable to do with regard to identifying human remains. Once these standards are developed, the state will need to train the Public Information Officer on these standards so no promises are inadvertently made to the public that the health professionals and government cannot deliver.

Issue 3 - The Commonwealth needs to establish a Family Assistance Center (FAC) plan with strict policies on the procedures for which agencies may accept reports on missing persons, what information is collected, who interviews the families on personal characteristics of missing/deceased victims of disasters, and who may receive the information. This will prevent confusion between the families and officials as well as prevent agencies from duplicating efforts and inadvertently providing conflicting information.

Recommendations

1. The FAC should be the only authorized site to collect information on missing persons via interview or password accessible website.

2. Identification and access to information will be limited to next-of-kin or a designated person assigned the password. The next-of-kin or designee should be fingerprinted for security and fraud prevention.

3. The DMORT Victim Identification Form will be used for information collection and to promote interoperability.

Issue 4 - The Commonwealth must continually educate the public and crisis event response teams on how to best deal with/respond to a mass fatality event.

Recommendations

1. Include OCME in meetings, drills, and working groups throughout the Commonwealth to allow fatality management and first responders to plan for and practice this portion of the exercises.

2. Should begin to connect with local EMS councils to begin the process of educating first responders on altering local medical examiners on a drill or actual incident.

3. Inform OCME of statewide exercise calendar and invite them to attend these drills.

4. Public Information Officers should be trained in educating the public, as well as state agencies, on how to best deal with a mass casualty event.

II. Attorney General Issues

Fraud Mitigation

Mass fatality incidents have historically resulted in fraud cases by some of the public. Lessons learned from the World Trade Center attack on 9/11 indicate fraud has been a major problem. Some examples of fraud that has occurred in past events are: persons assume new identities and their families report them dead/missing to receive entitlements, next-of-kin, survivors, and others have reported that "high valued" personal effects on their loved ones are missing and attempt to sue the state for the "return" of the items.

Issue 1 - How can the Commonwealth best reduce the risk of fraud following a mass fatality event?

Recommendations

1. The Family Assistance Center (FAC)/OCME should develop an online system of reporting. OCME will work with the Department of Social Services to develop this system.

2. The agency with the authority to receive reports should have legal authority to have families/persons, who are reporting missing persons, make sworn affidavits on the reports to allow for "false reports" follow-up.

3. A policy should be established limiting the agencies responsible for receiving missing person's reports to the FAC.

4. Reporters of missing persons, beneficiaries of entitlements, and those trying to claim personal effects should be required to provide identification and submit to fingerprinting for identification checks. *Everyone must ultimately report to the FAC for verification of status as next-of-kin.

5. To preserve personal effects and evidence, access to remains should be strictly limited to authorized persons who have crime scene and forensic documentation training to ensure personal effects are properly documented and recovered at scenes.

*Hospitals should be made aware of proper documentation of physical evidence for patients as well.

6. The OCME will liaison with the Cemetery Board to enable better coordination with them in the event of a crisis.

Issue 2 - The Commonwealth must be able to determine a clear and identifiable next-of-kin/legal guardian to ensure information is released to the proper people.

Recommendations

1. The Office of the Attorney General will provide a legal definition of "next-of-kin" and promulgate it.

2. Legislation may be necessary to identify who is legally in line to receive remains and personal effects of victims after a mass fatality event.

Property Disputes

Personal effects management will involve returning the effects to the legal next-of-kin. The likelihood of property disputes is high and the Commonwealth should prepare for how best to address these dilemmas.

Issue 1 -_ The Commonwealth should develop protocol for property disputes over personal effects from a mass fatality event.

Recommendation

Policies should be established for the identification of legal next-of-kin and the procedures to follow if disputes arise in the process.

Volunteers and Crisis Response Teams

The Commonwealth will need to address the various legal issues regarding liability protection for volunteers.

Issue 1 - Dentists, anthropologists, funeral service licensees etc. who respond and operate under the supervision of the OCME require a definition of status that would cover their person in the event of injury while responding to the OCME's request for assistance.

Recommendation

Clarify if volunteer workmen's compensation already exists and cite the Code section stating the same.

Issue 2 - Are OCME volunteer responders covered under the Volunteer Medical Liability Act passed by the General Assembly in 2005?

Recommendation

Clarify this in writing.

Human Remains

The Commonwealth needs to develop policy and procedure for the identification and disposition of human remains.

Issue 1 - Following a mass fatality event, various agencies will be required to collect and coordinate information to mitigate the situation. To accomplish this act, information, which is not normally shared or authorized to be released, will have to be released to accomplish the mission. Presumption has always been the OCME may request information from healthcare providers to assist with identification of deceased persons.

Recommendation

The Office of the Attorney General will clarify what information the OCME is legally permitted to request and obtain to identify physical remains from surviving as well as deceased patients, as limbs may be found that belong to people who survived the event.

Issue 2 - Bodies that are hazardous may need to be transported intra- and interstate for examination. What authorization is needed, if any?

Recommendation

The Office of the Attorney General will review the Code of Virginia for the ability of funeral service licensees or transporters to drive contaminated or highly suspicious remains over the roadways without Department of Transportation permits and placards.

Issue 3 - Mass fatality events will have unidentified body parts and some identified persons who will not be claimed. The Virginia Department of Environmental Quality, VDH, OCME and other responsible agencies should pre-identify possible locations where hazardous, unidentifiable or unclaimed remains may be interred.

Recommendations

1. Department of Environmental Quality, VDH, OCME, and other responsible agencies should pre-identify possible locations where remains could be interred for hazardous, unidentifiable, and unclaimed remains.

2. The Code of Virginia should also address how cemetery owners will be protected if the remains are safe for burial, yet considered to be "hazardous".

III. Budget Issues

Personnel Costs

The Commonwealth must ensure there are enough personnel to respond to a mass casualty event, and that the personnel are up-to-date with training for disaster response.

Issue 1 - What personnel expenses will the Commonwealth incur on a one-time and recurring basis?

Recommendations

1. The Commonwealth's number of medical examiners is dropping steadily with fee identified as a major issue. Local medical examiners are down from 430 in 1994, 283 in 2004 and 250 at present. The Board of Health considered medical examiner expertise, time and fee and recommended and authorized a fee increase to $150 per case. Requests for fee increase from General Fund failed to survive in 2005 in Governor's, House or Senate Budgets. The state should re-seek General Fund funding of fee increase. If General Fund will not support fee increase then ask for homeland security money or Tobacco Settlement money. Cost is $616,000 in first year with a recurring cost and estimated yearly increase of $30,000 for estimated increase of 200 cases per year at $150/case.

2. The Office of the Chief Medical Examiner needs 12 more investigators for direct reporting, 24/7 MED-X bioterrorism surveillance and investigation. System now has 8 investigators to cover 2 shifts weekdays. System fills in with part time fee for service day by day investigators. Learning curve is steep for intake screening, scene management and there is no follow-up by part-time investigators on case questions. Salary plus benefits, $70,000 x 12 = $840,000 (recurring). Requires 24/7

investigator coverage to receive information (see above) and a secure dedicated server: $15,000.

3. The OCME has 149 independent jurisdictions, 35 health districts, 6 hospital regions, 3 Metropolitan Medical Response Systems and over 100 military commands to interface with. The one current statewide planner is not physically capable of interfacing with all the drills and organizations despite numerous hours of overtime and traveling throughout the state. Thus the state should hire one additional Emergency Planner for OCME districts' training and planning to be stationed in highest risk area of Northern Virginia to work with Capitol Region Planners. Salary Plus Benefits $60,000 x 1 = $60,000 (recurring).

Preparation and Training Costs

Training and staffing will be required to properly operate the Family Assistance Center (FAC). To ensure efficient and effective management of this vital part of a mass casualty event response, the Commonwealth must budget for recurrent and one-time costs of readiness for the Department of Social Services (VDSS) and the Department of Mental Health, Mental Retardation and Substance Abuse Services (DMHMRSAS).

Not only does the FAC provide a means for securing essential information, it also provides either direct or referral services for the living family members who are seeking help for grief and mental health counseling, insurance questions, funeral guidance, financial assistance programs, social security issues, etc.. It is therefore, important that Commonwealth agencies authorized as lead for the FAC have adequate staff and training to serve the needs of the living.

Issue 1 - Virginia Department of Social Services (VDSS) needs 1 Planner and 1 Trainer to support its responsibilities in planning, exercising, developing procedures, and training staff. With the Department of Social Services serving as the lead agency for the FAC and DMHMRSAS serving as the lead partner, the addition of 2 staff, dedicated to emergency services, for each agency will improve our response and recovery efforts by insuring dedication of required time for planning and training for various responsibilities during mass casualty events.

<u>Recommendations</u>

1. VDSS will need the funds to properly train the people who are to staff and run the FAC in the event of a crisis. DSS cost of training and travel $400 x 50 staff =$20,000. One time cost of office set-up for 2 new staff = $8,000. Salary plus benefits and travel $65,000 x 2 = $130,000 recurring.

2. DMHMRSAS cost of training, travel, and revenue replacement lost due to staff being sent FAC training, $1500 x 110 (2 per community service board and 2 per facility) = $165,000. One-time cost of office set-up for 2 new staff = $8,000. Salary plus benefits and travel $150,000 x 2 = $300,000 recurring.

3. The Commonwealth should budget for recurring volunteer and local medical examiner training sessions, at $50,000.

4. The Commonwealth should budget for volunteer and local medical examiner background investigations, at $50/investigation x 350 = $17,500.

Travel and Equipment Costs

The Commonwealth will need to fund travel and equipment expenses to prepare for and respond to disasters.

Issue 1 - What travel expenses will the Commonwealth incur on a one-time and recurring basis?

Recommendations

1. The OCME will need vehicles for body transport and staff transport to use daily and during disasters. OCME is unable to use pool cars for day to day and transport (biohazard) usage, and will thus need 2 cars/vans $20,000 x 2 = $ 40,000 (One time, 5 year.)

2. The Command Center/Medical Examiner Response vehicle will need to be shared with the VDH and Vital Records. The VSP have been in the market for a used vehicle for OCME for some time. The state would incur a $300,000 (one-time) cost and a $3,000 yearly maintenance cost for this vehicle.

3. The Commonwealth should budget for $10,000 a year in operations travel for meetings with mutual aid states and for statewide training.

Issue 2 - What equipment expenses will the Commonwealth incur on a one-time and recurring basis?

Recommendations

1. Medical Examiner must ensure safety of those handling contaminated remains and safety of the public (Biowatch

Program). OCME will give a list to VDEM of supplies needed during mass fatality event. Keep a rotating store of supplies to get through 3 days of event until other supplies arrive. $75,000 (one time).

2. Storage must be an outside source accessible to the OCME. Buildings are at maximum capacity already with normal supplies. Rental costs: $1000/month (recurring).

3. Purchasing of WEB based communication equipment for interfacing with FAC, hospitals and EOC centers. The state should budget for a $100,000 (one-time) purchase of Web-EOC and other computer based information sharing equipment between hospitals.

4. OCME has no internal state resources for DNA identification services. Last plane crash, family paid for the DNA testing on the victims to get the remains released. Est. annual cost for normal DNA ID $10,000 at $500.00/test. For a disaster the cost could reach in the millions: NYC as of April 2005 $100 million on identification alone for the World Trade Center. The state will need a MOU with FBI or others to perform testing.

IV. Family Assistance Center (FAC) Issues

Coordination and Staffing

OCME staffing does not allow for the administration and management of a FAC. A lead agency is required to be identified with the appropriate legislative authority and funding to support such a function.

Issue 1 - The Commonwealth must designate a lead agency (authority) to form and coordinate the Family Assistance Center after a mass fatality event.

Recommendations

1. The Virginia Department of Social Services (VDSS) should be the designated lead agency in cooperation with the OCME for mortality matters.

2. Someone will need to designate VDSS as the lead. In addition the Dept of Mental Health, Mental Retardation and Substance Abuse Services needs to be designated as the secondary lead and all agencies within the Health and Human Services Secretariat need to be designated as responding agencies upon request.

3. If the language in the document designating the lead clearly states other agencies within the Secretariat will respond upon request, then it may be more appropriate for the lead agency to simply enter into MOUs with all agencies within the Secretariat.

4. Funeral Service Licensees can assist the FAC because they deal with families in these situations on a daily basis. They would be a good training resource.

Issue 2 - The Commonwealth should identify agencies that will provide staffing for a Family Assistance Center.

Recommendations

1. At the statewide level, all of the players need to be included into the planning and MOU's need to be established with the partners in the private and federal levels. Participants will include state, local, and federal agencies, as well as volunteer and private organizations.

2. Key agencies involved should meet to develop procedures.

3. Social Services and designated others need to be trained in completing the Disaster Mortuary Team Victim Identification Form that will be used to collect information at the FAC.

Preparation

It is imperative that the needs of the living are compassionately addressed, and the necessary public/private resources are appropriately trained and tools available if the FAC is to be a successful operation.

Issue 1 - What training will FAC personnel need to provide the best assistance to families affected by the disaster?

Recommendation

An organized and well-managed Family Assistance Center is the direct interface of the local governments and the Commonwealth of Virginia following any disaster. For the OCME it is essential to get the information from the families to identify the victims. Even if there are no deaths, the government must have a mechanism to efficiently provide services to the public. Grants or other funds should be found to provide all of the participating agencies the resources to develop and exercise FAC plans in Virginia.

Issue 2 - A data system is required to support a FAC for several purposes:

- To collect information on families and missing persons reporting their loved ones missing. Also allowing for web based reporting for those who cannot travel to the FAC.
- To track case histories on families and the services they received, are entitled to and what has been done or said to them before (this is to prevent victims from having to tell their story over and over again to each agency they encounter and to allow for caseworkers to see the history of each family's case. NTSB has a program such as this.).
- To provide information to the families and the public on the incident and services available (like the 211 system established), detailed information on the procedures each agency is doing (i.e. what is DNA and how is it collected and used in the identification process), the transcript of the family briefings given each day (MCI can do this as part of a contract with telephone bridges for those families who cannot travel to the FAC.)

Recommendation

The OCME needs to implement a tracking system that is interoperable with the Disaster Mortuary Team and National Transportation Safety Board to make Virginia forms as interoperable as possible.

Issue 3 - What equipment is needed for a FAC – who will fund, store, and set this up?

Recommendations

1. Establish a photographic identification card for processing for families and FAC workers with bar code tracking systems. This will enable the FAC to check in families to their stations, each employee interfacing with the families can be tracked in the case history and the location of families in the FAC can be easily traced, in case they are required to report somewhere for information or services.
2. Identify what VDH can do to connect OCME to hospitals to interface with their patient tracking systems.
3. A variety of office equipment will be needed (telephones, fax machines, etc.). Establish and fund the facility/space requirements for a FAC.

4. Determine if DHS will cover costs of a FAC operation if a federal declaration is received. FAC is not addressed in the National Response Plan.

V. Legislative Issues

Crisis Response Personnel

Currently only the full time staff of the OCME is identified as first responders in the smallpox immunization plan for VDH EP&R. Will this policy apply on all other first responder programs in the Commonwealth?

As defined in the December 17, 2003 *Homeland Security PresidentialDirective/HSPD-8*: " d) The term 'first responder' refers to those individuals who in the early stages of an incident are responsible for the protection and preservation of life, property, evidence, and the environment, including emergency response providers *as defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101*), as well as emergency management, public health, clinical care, public works, and other skilled support personnel (such as equipment operators) that provide immediate support services during prevention, response, and recovery operations."

Issue 1 - OCME and all supporting staff (Funeral Service Licensees, Dentists, Anthropologists, etc.) need to be legally identified as first responders in Virginia.

Recommendation

A provision should be made to allow for voluntary immunization when indicated and for prophylaxis as needed when managing medical examiner cases at the medical examiners request. Cost is to be determined.

Disposition of Human Remains

The state must determine how best to dispose of human remains and memorialize the burial so it will be more acceptable to the public.

Issue 1 - Following nearly every mass fatality incident, the government has erected a memorial for the deceased. Traditionally, those unidentified remains or "common tissues" which cannot yield a positive identification have received respectful final disposition in a way suitable to the surviving family members.

Recommendation

Pre-planning for this activity should be considered with a lead agency identified and policies developed on who shall serve on a board with the family representatives to determine what final disposition is best for the particular incident.

Issue 2 - The State Model Emergency Health Powers Act of December 21, 2001 gave good guidance for health departments and legislative bodies to address human remains disposition. This guidance was not addressed in any of the emergency declarations addressed in the last three annual legislative assemblies for the Commonwealth of Virginia.

Recommendation

Insert policy guidance into Virginia's Emergency Declarations.

Conclusion

Task Force Members identified insufficient Medical Examiner staff and budget to develop and support mass fatality management efforts in Virginia. The task force categorized its recommendations for improvement into four groups – administrative, Attorney General issues, budget issues, family assistance center issues and legislative issues.

The major administrative issue was insufficient staff in the Medical Examiner System and a fragmented death reporting system to support core activities for surveillance and crisis response. The task force recommends that 12 full-time examiners be established and funded to enable direct contemporaneous reporting of the half of Virginia deaths that occur out-of-hospital and implementation of screening by MED-X, the Center for Disease Control bioterrorism surveillance program for out-of-hospital deaths. Investigators would also be the on-scene medical management team for body recovery and evidence preservation. These positions would be part of the core of Virginia's own disaster mortuary operations team, a Virginia "DMORT".

A second major issue identified was the extent to which personal identification efforts would be carried out. The task force recommends that for closed events identification efforts would cease when all are identified, whereas for open events all recovered remains would be subject to scientific methods of identification.

Attorney General issues related to clarifying Virginia Medical Examiner jurisdiction with federal authorities, fraud mitigation and property disputes. The task force recommends working with Federal authorities to develop cooperative arrangements and asking the Office of the Attorney General to develop protocols to protect citizen survivors from fraud and safeguard personal property.

The major budget issue is the cost of recruiting and retaining Virginia Medical Examiners who are the front line city and county physicians who identify cases that are suspicious for bioterrorism (anthrax) and emerging infections (SARS, avian flu pandemic) and manage the grass roots death investigation system in Virginia. The numbers of Medical Examiners has declined from 430 in 1994 to 250 in 2004. The primary reason for resignation has been identified as the low case fee. The $50/case fee has not been increased since 1980, while Medical Examiners have been tasked with additional duties of surveillance, evidence collection and increased paperwork. The Board of Health approved an increase to $150 per case, which would require the General Assembly to allocate an additional $840,000 to the Medical Examiner System budget. The request was not included in any of the 2005 General Assembly budget documents.

Virginia has no family assistance center. The Virginia Department of Social Services has been tasked with establishing a center where families may report missing family members, provide identification information and receive the other supportive services needed in times of crisis. The Virginia Department of Social Services needs staff and budgetary support for core staff to develop a family assistance center.

Two legislative issues resulted in recommendations to amend the Code of Virginia. The first would establish medical examiners and supporting staff as "first responders," which would facilitate prophylactic immunization for bioevent mortality management workers. The second recommendation requests that the Virginia State Model Emergency Health Powers Act of 2001 be amended to provide guidance on the final dignified disposition of unidentified "common tissues" and to make provisions for memorials in honor of mass fatality victims of terrorism.

Performance Measures for Commonwealth Preparedness

Report & Recommendations of the
Performance Measures Task Force

Submitted to the Secure Commonwealth Panel

May 10, 2005

Table of Contents

Preface

The Secure Commonwealth Panel created this task force and charged its members with developing measures to gauge the performance of the Commonwealth and its localities in meeting the challenge of ensuring our overall preparedness in the area of homeland security. This report is our effort to meet this charge, and reflects the views of the task force members. In preparing this paper, we have drawn on the inputs of numerous experts in the Commonwealth, including government officials and individuals in the private sector and academia. We thank them for their important inputs. At the same time, however, we acknowledge that the responsibility for the contents of this report are our responsibility only, and not that of the organizations with which we are associated.

Thanks also go to Megan Stifel of Sutherland Asbill & Brennan and Mary Warder of the Office of Commonwealth Preparedness for their significant contributions and assistance in the preparation of this report.

Jeffrey P. Bialos
Task Force Chair &
Rapporteur

Members

Jeffrey P. Bialos, Chair
Partner, Corporate
Sutherland Asbill & Brennan LLP

Janet L. Clements
Deputy State Coordinator
Department of Emergency Management

BG (Ret.) Manuel R. Flores
State Director
Selective Service System

Dr. Lisa G. Kaplowitz
Deputy Commissioner for Emergency
Preparedness and Response,
Virginia Department of Health

Mike McAllister
Department of Transportation

Jan Sigler
Special Assistant to the Governor
Office of Commonwealth Preparedness

Staff
Megan Stifel
Sutherland Asbill & Brennan LLP

Dr. Vinton G. Cerf
Senior VP, Technology Strategy
MCI

Julian Gilman
Department of Emergency Management

Bobby Mathieson
Chief Deputy Director
Department of Criminal Justice Services

Yacov Y. Haimes
Professor, University of Virginia

Suzanne E. Spaulding
Managing Director, The Harbour Group
LLC

John S. Quilty
Retired, Senior Vice President and
Director MITRE Corporation

Capabilities & Performance Measures for Commonwealth Preparedness

One critical element of maintaining a "safe, secure and prepared Virginia" is to establish a set of performance measures to assess how the Commonwealth is performing in meeting its goal of "developing and overseeing a coordinated prevention, preparedness, response and recovery strategy for natural and man-made disasters and emergencies."[3] Performance measures can help in determining the effectiveness of the Commonwealth's preparedness capabilities, in improving their efficiency, and in allocating resources in support of the Commonwealth's goals.[4]

1. "Core" Preparedness Capabilities for Virginia

Establishing performance measures requires establishing a base line set of core competencies or capabilities Virginia must develop, in the short, medium, and long term to meet these preparedness goals (i.e., of maintaining an integrated homeland security and emergency capability). These capabilities must encompass all elements of the Commonwealth and its citizenry, including government, the private sector, and the public, and must take into account the relationship of the Commonwealth's activities to those of the federal government and other state governments.

In the early years after September 11, the Commonwealth's focus has been primarily on taking short and medium term measures needed to close clearly identified "capability" gaps rather than establishing a long term vision of Virginia's security and ensuring we have the right capabilities to meet those overall needs. Indeed, most of the federal homeland security grant assistance received by the Commonwealth has been utilized for specific equipment gaps that were identified rather than training and the development of overall capabilities or protocols. With the passage of time and the completion of many short term tasks, it is now time to plan for the longer term and put in place a full scale, integrated homeland security strategy, including the building of an integrated set of capabilities to prevent and respond to homeland security threats and a system of standards to measure whether Virginia is meeting its preparedness needs.

This report thus sets forth:

A(viii)[3] Consistent with these objectives, this memorandum addresses an "all hazards" approach (i.e., it encompasses performance measures designed to address the effectiveness of the Commonwealth's capabilities with respect to both homeland security threats as well as other disasters (man-made and natural). Thus, unless otherwise stated, the discussion herein, and the use of the term "preparedness" relates to "all hazards; the term "homeland security" capabilities or threats relates solely to such security threats and not to "all hazards."

A(ix)[4] There is a well established literature on performance measures, which highlight that they serve both external and internal agency purposes – in particular in assisting agencies to effectively and efficiently manage their operations and as part of strategic and operational management. See, e.g., Guide to Performance Measure Management, Texas State Auditor's Office, 7-8 (1999).

1) The core competencies we believe are needed in Virginia as part of an overall "enterprise" approach to developing and implementing a coordinated preparedness strategy for the Commonwealth.

2) Performance standards to measure the Commonwealth's performance in meeting the core competencies identified as intrinsic to preventing, preparing for, responding to and recovering from natural and man-made disasters and emergencies, including terrorist attacks.[5]

2. Key Considerations in Shaping and Measuring Preparedness Capabilities

In developing an enterprise vision of "core" capabilities and related performance measures for Virginia's preparedness, we believe that a number of factors are critical:

A. The Commonwealth homeland security "enterprise" is only one aspect of the overall holistic U.S., and ultimately, global approach to providing homeland security to the citizens of the Commonwealth and other U.S. and foreign jurisdictions. It is important to recognize the limitations of Virginia's role while ensuring that its efforts are fully integrated with, and draw maximum benefits from, those of other jurisdictions. Performance measures adopted for the Commonwealth must recognize the Commonwealth's specific role – and possible limitations – in performing these functions. Performance measures must also gauge the extent to which the Commonwealth and its localities have developed seamless intergovernmental relations that maximize Virginia's preparedness.

B. The Commonwealth homeland security "enterprise" must be consistent with federal government directives and guidelines, utilize appropriate tools provided by the federal government, and recognize and adapt to federal policies on the provision of homeland security grant assistance to states and localities. The enterprise "capabilities" must be developed within the framework of U.S. Homeland Security Presidential Directive-8 on National Preparedness ("HSPD-8") and other pertinent federal laws, regulations and policies. In particular, the Commonwealth must recognize the following:

- Establishment of the National Preparedness Goal. Pursuant to HSPD-8, the U.S. Department of Homeland Security ("DHS") is developing an overall "national preparedness goal" and defines "preparedness" as the "existence of plans, procedures, policies, training, and equipment necessary at the Federal, State, and local level to maximize the ability to prevent, respond to, and recover from" domestic terrorist attacks, major disasters, and other emergencies. The term preparedness, as used below with respect to the Commonwealth, incorporates this definition.

A(x)[5] For further definitions of these terms, see Homeland Security Presidential Directive-8.

- The Role of Risk Assessment in Homeland Security Planning. The federal government, including DHS, has endorsed the use of "risk assessment" as a critical element of homeland security planning, and has clearly articulated that it will, in establishing the National Preparedness Goal, "establish measurable readiness priorities and targets that appropriately balance the potential threat and magnitude of terrorist attacks, major disasters and other emergencies." HSPD-8, ¶ 6. Within this framework, DHS is now in the process of working with other stakeholders to develop a range of "all hazard" scenarios for use in homeland security risk planning and establishing specific "tasks" needed to address these priority scenarios. The Commonwealth and its local governments can and should review these scenarios and utilize them as tools to assess their own vulnerabilities and develop their own strategies.
- Federal Grant Funding Tied to Adoption of State Strategies. The President has directed that the federal government shall, to the extent permitted by law, predicate the provision of federal preparedness grant assistance to states on "adoption of Statewide comprehensive all-hazards preparedness strategies." HSPD-8 states that such state "strategies" should be consistent with the National Preparedness Goal, should assess the most effective ways to enhance preparedness, should address areas facing higher risk, especially to terrorism, and should also address local government concerns … ."
- Preparedness Requires Performance Measures. Finally, HSPD-8 states that the National Preparedness Goal will establish not only "readiness metrics," but "a system for assessing the Nation's overall preparedness to respond to major events, especially those involving acts of terrorism." As states and localities play a critical role in meeting national preparedness goals, establishing performance measures for these non-federal capabilities is critical to overall preparedness.
- Responding to Federal Alert Levels. The federal government has established a detailed level of alert procedures. The Commonwealth must have a procedure in place to respond to an increased federal alert level. At the same time, given the significant degree of critical infrastructure in Virginia, the Commonwealth must have a procedure to independently raise its alert levels to protect its citizens and infrastructure without relying on a change in the federal alert level.

C. Performance measures must be "living and breathing." Performance Measures must be periodically reviewed and updated to adopt to both changing threats, consequences, and vulnerabilities as well as changing federal standards of homeland security for states and localities (some of which are utilized as criteria for providing funding to states and localities).

D. Performance measures must be shaped for the Commonwealth and its local governments as well as for critical infrastructure, industry, and our citizenry. Performance measures undoubtedly will vary from one level of government to another and one industry to another. There is no "one size fits all." Local governments will face different types and degrees of risk and each local government will not be able to have in place a capability to guard against the full range of possible threats, including the range of high priority threats identified by DHS; this would be neither prudent nor cost-effective.

The performance measures recommended in this report are for the Commonwealth's state government (hereafter, the "Commonwealth) and its local governments. While the state is divided into regions for various administrative purposes, it is the province of local governments, with their legal authority, functions, budgets and personnel, to prepare for emergencies, declare states of emergency, request assistance and resources, and manage local emergencies.

In the public health arena, the picture is somewhat different; the Commonwealth's designated regions for public health purposes have some capability of their own and do play a role in emergency preparedness. It therefore is important to understand and measure the performance of the Commonwealth's regional public health capability.

E. Numerous existing performance measures should be utilized as appropriate. The federal government, numerous states and quasi-public or public standards bodies have created performance standards and measures for various aspects of the homeland security and emergency preparedness. These include federally-mandated rules for nuclear reactors and local governments in regions where they are situated, federal grant criteria that restrict eligibility for and use of funds, and private standards bodies that establish self-accreditation mechanisms in areas like state and local emergency management.[6] In developing homeland security performance measures for the Commonwealth, we have recognized that:

1. Some state functions are governed by federal law and grant conditions and criteria and these rules may provide sufficient measures of performance in some areas (but leave gaps in others);
2. Existing standards developed by expert bodies may provide useful benchmarks that the Commonwealth should utilize for its own self-measurement (rather than developing altogether new standards covering the same ground); and,
3. Standards utilized by other states and localities offer useful elements that can be drawn upon and adopted to Virginia's circumstances. In effect, the Commonwealth will utilize a "system of systems" of standards that draws as appropriate on elements of the existing standards in assembling an overall "enterprise" set of measures against which the Commonwealth's performance should constantly be measured.

A(xi)[6] In particular, the National Fire Protection Association 1600 Standard on Disaster/Emergency Management and Business Continuity Programs (2004) ("NFPA 1600 Standard") warrants careful consideration by the Commonwealth and its local governments.

F. Performance Measures should be as objective as possible and focus on important indicators of performance. Performance measures are a method of collecting, analyzing, and reporting information in order to track resources used, work produced, and attainment of desired goals. In the ideal world, we would be able to track success by reference to societal "outcomes" of our preparedness policies (i.e., what public benefits have been derived from the Commonwealth's actions). In other words, have the Commonwealth's preparedness capabilities in fact reduced its vulnerability to homeland security threats and natural disasters? Thus, we could measure success by the number of homeland security or emergency "events" that occur and societal costs that result. While this approach is useful where relevant, the reality is that there are few objective measures that exist and they do not tell the entire story. Measuring how many events have occurred and their social costs does not necessarily correlate to how prepared we are for such events, which can vary in nature, size, location, and scope.

Thus, performance measures also measure not only societal "outcomes," but the effectiveness of the government's capabilities in a given area – here, preparedness capabilities. This type of measurement focuses on "inputs" into government capabilities (agency resources, plans, personnel, and the like), the "outputs" of such capabilities (i.e., how many hospital beds are provided during an emergency), and the efficiency of government response (how quickly or broadly are such capabilities provided – i.e., how quickly are alleged incidents responded to, etc.).[7] Indeed, the bulk of the performance measures suggested below relate to capabilities rather than outcomes. However, it also should be recognized that these "capability" tools may not, in the real world, necessarily fully correlate with reduced vulnerability. We may, for example, enhance capabilities in some areas only to find that other areas then become targets of opportunity for terrorists.

Further, it should be recognized that the best performance measures are objective and quantifiable. While we have strived for this, there are difficulties in achieving this goal today. The new nature of the homeland security function makes it difficult to quantify performance in numerous areas at this time. For example, how many hospital beds do we need in a relevant geographic area? There are no clear answers to this today. The task force lacks sufficient information to form a judgment, and leaves further quantification to experts and to the development of more experience in this area. Further, as a sign hanging in Albert Einstein's office at Princeton University said: "Not everything that counts can be counted, and not everything that can be counted counts." Thus, we must take this useful advice into account and avoid reliance on easily quantifiable measures simply because they are quantifiable. How quickly the

A(xii)[7] For a useful overview of performance measures, see Guide to Performance Measure Management, Texas State Auditor's Office, 7-8 (1999).

Commonwealth processed incident reports may be readily observed but may not be an adequate gauge of our preparedness.

Thus, the performance measures below are mostly non-quantifiable in nature and are designed instead to focus on the right areas where measurement is warranted. We have left it to experts in state government to develop more precise and quantifiable measures of these areas in the months and years to come.

G. Performance measures should be realistic and established with relevant time horizons in mind. Setting enterprise-level performance measures must take into account the realities of constrained budgetary and personnel resources as well as legal and governmental processes. It would make little sense to establish a set of performance measures, for example, that are unachievable due to the enormous resources required. Thus, measures must be established that are attainable in the short, medium, and long term. Many of the capabilities set forth in this report are not fully in place or operational today; they are works in progress or likely to be established over the next few years.

H. Performance measures should not only measure what capabilities are "put in place," but the degree of implementation and effectiveness of the capabilities. Understandably, a major focus of performance measures, especially in this initial period of development, is on assessing whether the core capabilities are put in place. At the same time, however, it is important to capture and measure, to the extent possible, not only the establishment of such capabilities, but also whether they are operational and effective. Undoubtedly, as discussed below, exercises will be part of this effort, especially in the area of measuring response to incidents. But other measures also may be necessary in the areas of prevention and detection. As time goes by, and more capabilities are put in place, implementation and execution will become the focus of measuring preparedness.

3. Identifying Areas for Performance Measures

In order to assist the Commonwealth in developing performance measures, we have identified particular capability areas and sub-areas that should, in our view, be measured; the list is not meant to be exhaustive but rather exemplary. We suggest key measurements in each capability area that should be reviewed by experts and, subject to their judgment, made more quantifiable or detailed as appropriate.

With these considerations in mind, the following are the subject areas in which performances measures are appropriate relative to homeland security capabilities:

A. General Capabilities:

1. Laws & Authorities

2. Accountability & Organization
3. Planning/Risk Assessment Function
4. Budgetary Transparency & Accountability
5. Grant Functions (Grantor & Grantee)
6. Intergovernmental Relationships
7. Continuity of Government

B. Specific Functional Capabilities:

- Communications
- Critical Infrastructure
- Emergency Response
- Health & Medical Preparedness
- Information Sharing
- Information Technology Security
- Law Enforcement & Criminal Justice
- Mutual Aid
- Private Sector Preparedness
- Public Awareness
- Recovery
- Training & Exercises
- Transportation

C. Support Capabilities - The Focus on Training:

In each of these areas (general and specific functional capabilities), it is important to assess whether the Commonwealth and its localities have in place sufficient supporting capabilities, as reflected in:

1. Plans, procedures and strategies;
2. Funding (whether from budgeted funds, grant assistance or otherwise);
3. Assigned personnel; and
4. Training.

Given the relatively new and developing nature of the homeland security and preparedness capability, it is particularly critical to fund training at all levels of government. The presence of adequate and ongoing training – has the government unit assessed its training needs, identified personnel requiring training, secured resources for it, and proceeded to conduct the training – is a critical performance measure.

Thus, whether explicitly mentioned or not, each of the performance measures set forth below should be assumed to include, as a sub-element, these support capabilities.

4. Commonwealth Preparedness Capabilities & Performance Measures

A(v) Below we set forth recommended performance measures. We have crafted these measures in terms of a general question, which are designed to serve as an overall introduction to the particular subject and capture the overall performance objective. The more specific "sub-elements" that follow each question comprise the performance measures designed to answer the question.[8] Finally, where appropriate, we have provided a comment section designed to illustrate key challenges and issues and steps the Commonwealth has taken in various areas.

A. General Capabilities & Measures

I. Laws & Authorities

Do the Commonwealth and its local governments have in place the necessary laws, regulations and other measures needed to provide the broad ranging authority necessary to meet the Commonwealth's preparedness goals?

Sub-Elements:

- Does the Commonwealth, and its local governments, have in place an effective, and institutionalized, process to periodically evaluate existing laws, regulations, codes, and other authorities to determine whether adequate and flexible authority exists to meet its preparedness goals and accommodate homeland security developments?
  - Have the Commonwealth and its local governments addressed the legal "gaps" identified through such a process to date?
- Does the Commonwealth's process for addressing legislative "gaps" bring together all stakeholders and take into account the full range of potential impacts of such legislation, including budgetary costs, burdens on the private sector and the public, and issues concerning privacy and the treatment of proprietary private sector information?
- Does the Commonwealth have a long term "gap" strategy to address the need for legislative and regulatory revisions?
- Do Commonwealth agencies and entities that have the authority to conduct emergency operations have authority to take action prior to an event to mitigate the occurrence or recurrence of the event?
- Does the Commonwealth's evaluation of exercise results (see Performance Measure VII, "Continuity of Government," below) consider the need for and impact of changes to laws, regulations, and or legal authorities?

Comment: The Secure Commonwealth Panel and the Governor's Office of Commonwealth Preparedness ("OCP") have together played critical roles in identifying and shaping legislation to fill "gaps" in preparedness authority.

A(xiv)[8] While we recognize that performance measures generally are phrased as declaratory statements rather than questions, the distinction is not a substantive one. These questions can easily be rephrased.

However, neither the Panel nor OCP are institutionalized entities, and both, created by executive order of Governor Mark Warner, will expire at the end of his term. Accordingly, a permanent process should be developed to review state laws and regulations pertaining to security and preparedness on an ongoing basis. See also the Comment to Performance Measure II, "Accountability and Organization," below.

II. Accountability & Organization

Do the Commonwealth and local governments have clearly established lines of authority for "all hazard" preparedness that specifies which units of government and individual positions are responsible for particular functions,?

Sub-Elements:

- Does the governmental entity have a unit or individual in charge of coordinating all of the elements of the multi-disciplinary, multi-agency preparedness function?
- Does each agency or other preparedness function at the state and local level have written protocols in place for cooperation with other governmental entities?
- Does the allocation of authority for homeland security functions reflect an efficient,
  effective, and equitable balance of responsibility and authority among the government entities?

Comment: The Commonwealth's experience dealing with emergency situations in recent years has highlighted the critical need for clear lines of authority and accountability for not only such events, but for the forward planning needed to deter, prepare for, and recover from such unfortunate events. The role of the OCP has been vital in shaping a holistic approach to preparedness for Virginia. The members of this task force find that there is a vital need for a central coordinating entity for long-term security and preparedness in the Commonwealth. It therefore is the recommendation of this task force that OCP, which currently exists by virtue of executive order that will expire in accordance with the terms of such order, should be made permanent by the General Assembly during its next session.

The task force recommends that the General Assembly provide the coordinating office it creates with broad authority to manage and coordinate the homeland security function for Virginia, with responsibility to identify and fill legal gaps in authority, prepare and address budgetary needs (working in coordination with other state departments and agencies), allocate federal grant assistance where such decisions are discretionary (or supervise its allocation by responsible state departments or agencies), and work with the federal government, other states, and local governments to develop and implement a preparedness strategy for the Commonwealth.

The task force recommends that the continued need for a Governor-appointed panel for security and preparedness also should be considered by the General Assembly. While there is considerable merit and utility to this approach especially in the formative period, when it is important to bring all stakeholders to the table and shape the initial approach, at some point its functions should be institutionalized whether through OCP or a separate advisory board.

III. Planning/Risk Assessment Function

Does the Commonwealth, or local government, have a plan and planning mechanism that reasonably addresses its "all hazard" preparedness goals (including prevention, response, and recovery)?

Sub-Elements:

- Is the plan, and its proposed elements, priorities, and resource allocations, based on a reasoned assessment of overall risks that takes into account possible threat scenarios (including the planning scenarios recently promulgated by DHS), the likelihood that such scenarios could occur in the relevant geographic area, the magnitude of such potential incidents, and potential consequences and costs?
    - Has the governmental unit identified potential hazards and inventoried facilities or locations where risks exist?
    - Does the planning process and resulting plan appropriately utilize the hazard identifications and risk assessment methodologies set forth in the National Fire Protection Association 1600 Standard on Disaster/Emergency Management and Business Continuity Programs (2004) ("NFPA 1600 Standard")?
    - Has the Commonwealth or local government undergone the DHS Office of Domestic Preparedness' Homeland Security Assessment?[9]
    - Do all local governments have mitigation plans that meet the standards of the federal Disaster Mitigation Act of 2000[10], which established a requirement that local governments have mitigation plans in order to be eligible for federal grant funds, including the Hazard Mitigation Grant Program?
- Did the government entity consult with all relevant stake holders in developing its plan, including governmental, police and law enforcement, fire, emergency response, transportation, health and medical, military affairs, and the private sector?

[9] See http://www.shsasresources.com.

A(xv)[10] Pub. L. No. 106-390, 114 Stat. 1552.

- Is the plan periodically reviewed and revised to take into account changing DHS and other federal standards, planning scenarios, vulnerabilities, resources, and other factors?
- Does the government entity have the appropriate personnel, budgetary resources, and analytical tools to properly conduct efforts A-I, in Section 2 "Key Considerations in Shaping and Measuring Preparedness Capabilities," above?

Comment: Population size and concentration is certainly a relevant consideration in risk based planning, including, for example, in evaluating consequences of potential threat scenarios and allocating resources to address these threats. See HSPD-8 (directing federal departments and agencies, in providing first responder preparedness assistance, to base its allocations on "assessments of population concentrations, critical infrastructures, and other significant risk factors … .").

Members of the task force recommend that the Commonwealth develop its security and preparedness plan and allocate resources on the basis of an assessment of "risks" and not on the basis of a pre-ordained or automatic formula based on population. Artificial and non-risk based formulas should not be utilized by the Commonwealth in preparedness planning.

IV. Budgetary Transparency & Accountability

Does the Commonwealth or local government have the budgetary resources to meet its identified preparedness needs?

Sub-Elements:

- Does the unit of government have:
    - Transparent records of its past total spending on preparedness and funding sources;
    - A projected budget for the future – at least two years, together with a written list of funding sources, when known; and
    - A mechanism for tracking the spending and use of federal grant funds?

- Have all possible funding sources been identified, including the use of tax benefits?

Comment: The availability of federal grant assistance generally is generally only known a year in advance. Thus, budgets beyond one year would be somewhat notional but are helpful to encourage long range planning by government units. However, where possible, it is important to have predictable funding streams (whether through multi-year federal grants or multi-year Commonwealth appropriations of funds).

V. Grant Functions (Grantor & Grantee)

Has the government entity expeditiously, reasonably, and transparently allocated and/or expended grant funding related to its preparedness functions from the U.S. government and other sources?

Sub-Elements (Commonwealth):

- Has the Commonwealth developed one or more fair, reasonable, and transparent mechanisms for distributing federal grant assistance to local governments, and has it utilized this mechanism in practice?
- Does the Commonwealth take into account the performance of local governments under the performance measures noted herein in distributing such funding?
- Does the Commonwealth utilize the risk assessment methodologies in distributing funding rather than solely relying on population or other criteria? (see the Comment on Performance Measure III, "Planning Risk Assessment Function," above)
- Does the Commonwealth have an adequate capability to review and measure the performance of local governments in taking their performance into account in distributing funding?

Sub-Elements: (Commonwealth and other local government recipients of grant funds):

- Do local governments that receive grant funding disperse such funding efficiently and expeditiously?
- Have local governments that have sought grant funding for the acquisition of equipment funded the resources necessary for training in the use of such equipment?
- Does the Commonwealth or government entity, have a mechanism in place to address identified, but unfunded needs and to ensure appropriate funding in the future?
- How many local governments did and did not receive grants in each of the last three years? Why did some governments not receive funding, and what is the consequence of the lack of support?

Comment: While we have been unable to quantify with precision how much of the Commonwealth's preparedness funding is from federal grant assistance (such data is not readily available at this writing), it is clearly the case that federal grants are the primary source of such funding. Accordingly, it is critical that the Commonwealth and its local governments be accountable for the distribution and use of such important funding. The federal grant assistance criteria change from time to time, and vary from one functional area to another. Nevertheless, it is vital that the Commonwealth maintain its own disciplined approach to exercising its discretion, where it exists, to allocate funding within the state within the parameters of federal grant criteria. Such methodologies should be in written form and consistently applied (as they are in the health area today).

As a significant percentage of funding is for equipment at the local level, it is equally important that localities have assessed training needs with respect to such equipment and funded and performed such training. It is of little utility to maintain equipment that will go unutilized in an emergency.

VI. Intergovernmental Relationships

Does the Commonwealth and its localities have the intergovernmental relationships necessary to ensure Virginia's preparedness?

Sub-Elements:

- Have the Commonwealth and localities forged strong intergovernmental relationships in critical preparedness mission areas (including, among others, intelligence and warning, transportation security, critical infrastructure protection, and public health) that can facilitate the cooperation, coordination, and collaboration necessary to ensure a safe, secure and prepared Virginia, including:
    - Vertical relationships – relationships between federal, state and local entities;
    - Horizontal relationships – coordination between similar state or local government entities; and
    - Geographic relationships – relationships with bordering states.
    - Do the preparedness plans, funding mechanisms, policies, and procedures of the Commonwealth and its localities contain elements designed to foster intergovernmental cooperation, coordination and collaboration? Do the Commonwealth's preparedness goals, plans and strategies include intergovernmental or interjurisdictional elements;
    - Do the procedures and protocols on intergovernmental activities reasonably cover activities needed for all elements of preparedness (prevention, preparation, response, and recovery), including:
        - preparation and implementation of preparedness plans and strategies;
        - sharing of intelligence and other relevant information (including local vulnerabilities); and
        - areas where mutual aid plans and procedures are put in place.
    - Are appropriate mechanisms for intergovernmental communications established?
        - Are there common protocols and designated primary and secondary points of contact known to and understood by relevant units of government?

        - Are there regular and ongoing communications between these entities?
- Has the Commonwealth, and its local governments, developed, articulated and implemented a shared vision with respect to intergovernmental relationships? Do governmental entities in the Commonwealth:
    - routinely identify specific and timely opportunities for intergovernmental action and innovation in support of their own preparedness goals and those of other relevant governmental units;
    - look at issues holistically;
    - build on previous successes in cooperation and collaboration for longer-term collaborative efforts; and
    - routinely identify main stakeholders, potential partners, and other affected parties and collaborate with these entities; and routinely incorporate intergovernmental relationships in their day-to-day operations?
- Does collaboration encompass all phases of the goal – planning, funding, approval, implementation, training, exercises and maintenance?

Comment: There are often strong governmental tendencies (institutional and cultural) and citizen desires to maintain the independence and prerogatives of existing governmental entities. Efforts to enhance coordination and collaboration must seek to re-orient existing entities and structures so as to ensure that effective intergovernmental relationships are integrated into and become part of the organization’s goals, missions, and structures.

The National Capital Region (“NCR”) presents a unique challenge for coordinating regional and intergovernmental planning, cooperation, preparation and response for the multiple government entities responsible for its over 4 million citizens and institutions. The NCR is comprised of the leadership of the District of Columbia, State of Maryland, and the Commonwealth of Virginia. Virginia has several representatives on the NCR’s Senior Policy Group.

The NCR has made significant progress in meeting the complex challenges of risk management, homeland security, and preparedness and has set an example for regional planning and coordination and responsiveness. This regional, intergovernmental coordination resulted in an NCR better prepared and more secure with a needs-based regional strategy for risk management, improving preparedness and addressing security.

VII. Continuity of Government

Is there a written plan to ensure the continuity of key governmental functions and facilities at the Commonwealth and local level during a homeland security incident or natural emergency?

Sub-Elements:

- Are there laws, regulations, or procedures in place for:
  - the declaration of a state of emergency; and
  - succession of key executive branch and legislative personnel?
- Has the unit of government identified the critical, time-sensitive records and data ("critical data"), and government functions and processes that must be maintained during emergencies;
- Is there a written plan sufficient to ensure the continuity of critical records and government functions during an emergency?
- Do the continuity plans provide for their periodic review to ensure that they remain current?

Comment: The Commonwealth has had plans in place for a number of years that have evolved over time, including plans for high level succession planning. More steps are needed to ensure continuity of governmental functions and critical records at the local government level.

B. Specific Functional Capabilities & Performance Measures

VIII. Communications

Does the Commonwealth have sufficient, reliable and inter-operable communications systems (internally and with the federal government and other states and entities as appropriate)?

Sub-Elements:

- Are there redundant communications systems in place should one system fail?
- Are the Commonwealth's systems and those of its local governments inter-operable with one another and do they allow adequate and reliable communications between each other and with federal officials?
- Does the Commonwealth, and its local governments, have a reliable procedure to notify officials and emergency response personnel potentially impacted by an actual or impending emergency?
- Is the Statewide Agencies Radio System ("STARS") program on schedule for completion? What percent/number of local governments will participate in STARS?
- Does the Commonwealth, and its local governments, have the capability to meet all elements of its emergency response plans?
- Are written protocols, processes and procedures in place at the state and local level for communications during emergencies?
- Does the Commonwealth have in place an adequate Emergency Alert System ("EAS") that can notify the public potentially impacted by an actual or impending emergency?

Comment: By Executive Order 28 (2002), Governor Warner established a program to develop the STARS system of integrated radio and wireless data communication for state agencies engaged in public protection and safety and for the mutual aid needs of state and local law enforcement agencies. The STARS program recognizes the need for a shared, statewide, public safety-grade radio system that includes law enforcement mobile data, and facilitates interoperability between state and local police communications systems at the city or county level. STARS will replace the existing analog communications system used by the Virginia State Police and other state agencies with a VHF digital high-band trunked system that integrates radio and wireless data communications. The Commonwealth has entered into a contract for the procurement of the system and it is expected that the system will be partly operational in 2005 and fully operational by 2009.

IX. Critical Infrastructure

Are adequate protections in place for all portions of the Commonwealth's infrastructure identified in the National Asset Database as "critical" including utilities, nuclear facilities, commercial assets, and others?

Sub-Elements:

- Are all potential critical infrastructure sites identified by the units of government in which they are located?
- Has a buffer zone protection plan ("BZPP") been established for each identified structure or location?
- Has the BZPP been exercised and have security audits been conducted in order to ensure feedback?
- Is there a plan to handle multiple site incidents?
- Are the consequence zones, or inter-dependencies of any particular site cross-jurisdictional? If so, are mutual aid measures in place?

Comment: Under the U.S.A. Patriot Act,[11] the term critical infrastructure refers to those "systems and assets (resources), whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety or any combination of those matters." The DHS Protective Security Division builds the National Asset Database from thirteen sectors and four key resource areas. The sectors include: agriculture and food; water; public health; emergency services; defense industrial base; information; telecommunication; energy; transportation; banking and finance; chemical and hazardous materials; postal and shipping; and national monuments and icons. DHS also utilizes the following four key resource areas: nuclear power plants; dams; government facilities; and commercial assets.[12]

The BZPP program provides funding to reduce vulnerabilities of critical infrastructure ("CI") and key resource ("KR") sites by extending the protected area around a site - thus creating a further protection in the surrounding community. The DHS Information and Analysis and Infrastructure Protection (IAIP) division, in participation with state and local officials, reviews vulnerability assessments to identify security needs. The BZPP program is

[11] Pub. L. No. 107-56, 115 Stat 272. See also Homeland Security Presidential Directive – 7 (specifically defining and enumerating the critical infrastructures in the United States) (see http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html).

[12] See also Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection (Oct. 1997). See also Homeland Security Presidential Directive – 7 (specifically defining and enumerating the critical infrastructures in the United States) (see http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html).

administered by staff assigned to the Security & Emergency Management Division (Transportation Protective Security), of the Virginia Department of Transportation, in direct support of the Office of Commonwealth Preparedness. The program involves liaison with local law enforcement and owners/operators of CI/KR sites throughout Virginia, in order to continue to safeguard our nation and minimize the potential for a terrorist attack. The BZPP helps local authorities assess current vulnerabilities at identified critical infrastructure and key resource sites, and develop and implement plans to increase the level of protection, while acting as a deterrent and prevention mechanism of possible terrorist threats or incidents. In developing these plans, responsible jurisdictions review and assess ways in which they can work with relevant federal, state, local, tribal, and private sector agencies to coordinate their prevention activities.

X. Emergency Response

Does the Commonwealth, and its local governments, have the capability to oversee and coordinate a timely and comprehensive response and recovery plan for man-made and natural disasters?

Sub-Elements:

- Have the Commonwealth, and its local governments, been accredited by the Emergency Management Accreditation Program ("EMAP")?
- Have local governments conducted self-assessments using the Local Capability Assessment for Readiness ("LCAR") self-assessment instrument and used the results to strengthen capabilities?
- (for the Commonwealth) How many of Virginia's local governments have been accredited under EMAP and/or self-assessed under LCAR (in percentage and absolute terms).
- What departments and agencies within the Commonwealth are designated as emergency responders? What level and type of emergencies will warrant the request for assistance from the federal government (e.g., National Guard) and private organizations?

Comment: While the EMAP accreditation process is effective, the process is expensive and lengthy and, hence, may not be a viable alternative for localities in the absence of grant assistance. Thus, task force members recommend that LCAR self-assessments are a reasonable alternative to EMAP accreditation approach.

XI. Information Sharing

Does the Commonwealth have access to all relevant information, including intelligence from the federal government and a fusion process to evaluate and disseminate relevant information and intelligence to state, local, and the private sector?

Sub-Elements:

- Has the Commonwealth identified all key sources of relevant information, including sources within the private sector?
- Have policies and protocols been developed for gathering and sharing of information?
- Have state and local personnel been trained to recognize relevant information, gather it appropriately, and disseminate it in a timely fashion?
- Has the Commonwealth identified all entities, including within the private sector, to whom relevant information should be disseminated?
- Have appropriate policies and protocols been developed to ensure the widest possible access to, and sharing of, information consistent with the need to protect classified information, sensitive law enforcement information, and privacy and due process rights?
- Do the Commonwealth's fusion process/Fusion Center and Emergency Operations Center ("EOC") have clear missions and strategic plans?
    1. Are the Commonwealth's fusion process/Fusion Center and EOC adequately and appropriately staffed, including by personnel from agencies with relevant informational needs and capabilities?
    2. Do the Commonwealth's fusion process/Fusion Center and EOC maximize participation by and information sharing with state and local governmental entities?
- Does the Commonwealth have the capability to communicate and store classified information in compliance with Federal standards?

Comment: The Virginia Fusion Center has been stood up to address many of these issues. It is expected to become operational within the very near future. The concept of the Virginia Fusion Center is to bring key critical response elements together in a secure, centralized location so that information and resources can be shared in order to provide a well-orchestrated and coordinated intelligence function. The information will be collected, prioritized, classified, analyzed and disseminated in order to better defend the Commonwealth against terrorist threats and/or attack. The Virginia Fusion Center should be operational in the autumn of 2005. It is the intent that all relevant terrorism information and intelligence be centralized and directed or legally mandated to be processed through the Center.

At the same time, however, it should be recognized that the Fusion Center cannot provide all needed capability nor be a substitute for maintaining necessary Commonwealth functions of detection, investigation, surveillance, and others related to identifying and preventing potential homeland security threats.

XII. Information Technology Security

Does the Commonwealth have an effective information technology ("IT") security plan?

Sub-Elements:

- Is there an agency or person responsible for Virginia's IT security? Is that agency or person in contact with relevant private sector entities so that threats to each are shared quickly and appropriately?
- Are reports of cyber attacks in the Commonwealth tracked and is a responsible agency in charge of addressing them? Have the number of reports increased or decreased in the last year? Is there an agency within the Commonwealth that reports cyber incident statistics to the Software Engineering Institute (SEI) and are there collaboration opportunities that exist between the Commonwealth and SEI?
- Have rules and procedures been put in place to facilitate the supply of such information to the Commonwealth and, as appropriate, its local governments, by the private sector? Are policies and procedures in place to ensure that all information technology systems (the Commonwealth and its local governments) receive critical security updates in a timely manner?
    - Is there a program that provides regular testing of information technology systems to audit and report whether they have received critical security updates?
- Have rules and procedures been put in place by the Commonwealth and its local governments to require the assessment and mitigation of risk in all information technology systems that store, process, and transmit sensitive data?
    - Do such policies and procedures include requiring acceptance of any residual risk by Executive management?
    - Do such policies and procedures require that any and all new information technology systems are reviewed prior to deployment to ensure that they meet Commonwealth technology architecture standards, including security standards?
- Have all Commonwealth personnel who use information technology resources received basic security awareness training?
    - Have Commonwealth personnel with additional information technology responsibilities received advanced security awareness training commensurate with their responsibilities?

Comment: In this area, like others, it is critical to forge a partnership between government and the private sector. For businesses to share information about cyber attacks with the Commonwealth, there must be a sufficient degree of trust involved – i.e., does the Commonwealth adequately protect the known vulnerability of an entity to cyber attack such that such entities are willing to share such information with state government. Thus, it is imperative to establish modalities for these types of information sharing that limits access to this information to those in state government with a "need to know" and takes steps to ensure that this information is adequately safeguarded against inadvertent release.

XIII. Law Enforcement & Criminal Justice

Does the Commonwealth have an effective capability to develop and utilize all available information to deter, detect, and prosecute individuals and groups that cause homeland security threats?

Sub-Elements:

- Does the Commonwealth have the means to gain access to all relevant intelligence from the federal government, classified or otherwise, and all other relevant information (developed in-state or otherwise), and appropriately fuse, evaluate, and disseminate as needed such information to appropriate Commonwealth, state and local personnel? (See Performance Measure XII**,** "Information Technology Security," above for details).
- Does the Commonwealth have the capability to deal rapidly with "tips" and potential threats, including expedited analysis and investigation, real time sharing of information with federal authorities and others as appropriate, and development of quick responses?
- Does the Commonwealth and its local governments, and police and other law enforcement personnel, have in place procedures and protocols for acting to deter and detect homeland security threats?
    - Are the protocols and procedures coordinated and integrated among all affected entities, including those that have not participated in homeland security matters in the past?
    - Does each participating partner understand its mission and requisite operational purpose?
- Do the Commonwealth and its local governments have trained personnel and funding needed to carry out such activities?
    - Are agencies required to provide training for their personnel and is training identified as a priority for both preparedness as well as for budgetary planning purposes?
    - Are adequate funding streams in place in order to fulfill necessary training? (recognizing that federal grant assistance generally *cannot* be used *in place of* state funds but may only supplement state funds.)
- Does Virginia's judiciary have in place procedures and protocols to deal with sensitive information in carrying out prosecutorial functions relative to homeland security?

Comment: The task force understands that certain law enforcement entities, including the Virginia Sheriffs, in the past have received federal grant assistance that have enabled them to accomplish many of the objectives set forth above. With this funding, the Sheriffs' Association established a Terrorist Information Coordinator that served a valuable role in facilitating communications between law enforcement personnel. However, funding under that grant will no longer be available after August 2005. The task force therefore recommends that the Commonwealth make available funds in order to continue the progress of the Virginia Sheriffs and consider bringing the program under the auspices of the Virginia Fusion Center.

Similarly, the task force recommends that the Commonwealth avoid stove piping with respect to law enforcement intelligence and information sharing – the costs can be significant. In this regard, communication should be improved between relevant law enforcement entities in the Commonwealth to ensure that various intelligence gathering and dissemination mechanisms are properly utilized and coordinated.

XIV. Mutual Aid

Has the Commonwealth, and its local governments, utilized mutual aid agreements in their security and preparedness plans to maximize use of available resources?

Sub-Elements:

- Do the Commonwealth and local governments take the availability of assistance from other jurisdictions and entities into account in developing preparedness plans?
- Does the Commonwealth have mutual aid agreements in place with other states to help provide "surge" assistance in the event of a homeland security incident or natural disaster?
- Is the Commonwealth a participant in the nation-wide Emergency Management Assistance Compact ("EMAC")?
- How many local governments within the Commonwealth have mutual aid agreements in place with other governmental units and private sector businesses (in percentage and absolute terms)?
- Is the Commonwealth, and its local governments, aware of existing mutual aid agreements in place relevant to their territorial jurisdiction that would be activated in the event of an emergency?

Comment: The Commonwealth was one of the first members of the nation-wide Emergency Management Assistance Compact that includes most U.S. states and territories and has in fact received as well as provided EMAC assistance. Most of Virginia's 140 local jurisdictions are signatories to the Statewide Mutual Aid System, which has successfully been used in disasters.

XV. Private Sector Preparedness

Is the role of the private sector integrated in state and local security and preparedness plans? Do private sector entities in the Commonwealth have in place plans and processes to ensure their "all hazards" preparedness?

Sub-Elements:

- Do private sector businesses in Virginia have a process, supported by senior management and funded to ensure that the necessary steps are taken to identify potential risks to their facilities and the impact of potential losses, establish appropriate safeguards (physical and information security, etc.), maintain viable recovery strategies and plans, and ensure continuity of services?
    - Do such "continuity of business plans" consider the specific areas set forth in the NFPA 1600 Standard, Annex A, A.5.7.2.5.
- Do private sector businesses engage in personnel training, plan testing and maintenance, and undertake self-assessments of their preparedness?
- Has the Commonwealth, and its local governments, identified key private sector businesses critical to ensuring ongoing continuity of basic services to its citizenry and worked with those businesses to ensure continued service in case of a disaster or emergency?
    - Does the Commonwealth promote and participate in joint training and exercises with the private sector?
- Have the Commonwealth and its local governments, worked cooperatively with the private sector to: 1) identify private sector resources that can be used in responding to specific emergencies, and 2) agree upon and put in place mechanisms to ensure access to those resources in the case of such emergencies?
- Have at risk industries such as utilities, water treatment facilities, and chemical and nuclear plants established voluntary codes that specify preparedness and precautionary measures?
- Does sufficient sharing of information occur between the Commonwealth and the private sector regarding critical preparedness missions, and are there steps in place to enhance and improve such information sharing?
- Do private sector businesses in the Commonwealth have sufficient awareness of the State's Emergency Response Plan and the steps businesses are advised to take in connection with different terrorist threat conditions (as set forth at http://www.commonwealthpreparedness.virginia.gov/SecureVa/vathreat.cfm) ?
- Do private sector entities have effective information technology security plans and protocols for sharing information concerning IT incidents with the Commonwealth and its regions and localities? See Performance Measure XII, "Information Technology Security," above.

Comment: The private sector should be treated as an integral component of the Commonwealth's preparedness planning and response. The private sector must be a partner in every aspect of preparedness planning including information sharing, participating in exercises and recovery strategies. Private sector firms bring many specialized skills, unique talents and resources to the table that should be harnessed by the public sector for emergency situations. Such capabilities as electric power line crews, fiber optic repair teams, fuel transport, specialized construction and excavation can be very useful in responding to an event.

Processes and metrics exist in many Commonwealth industries (especially those that qualify as critical infrastructure and are subject to federal or state regulation) and should be utilized where appropriate.

XVI. Public Awareness & Warning

Is the public knowledgeable of state and local preparedness goals? Are there mechanisms in place by which the public is timely notified of emergency situations, what emergency actions should be taken, and the state and local response and recovery plans?

Sub-Elements:

- Does the Commonwealth, and its regional and local governments, have procedures and protocols for disseminating information to the public, the media, the private sector, and volunteer organizations with respect to each of the following:
  - the prevention of emergency events;
  - what steps to take if an emergency occurs; and
  - what to do during the recovery phase?

- Do these plans take into account and balance:
  - Differences between the types of homeland security needs (prevention, preparedness, response, and recovery) and the different public groups and localities; and
  - Considerations of timing, potential public impact of announcements, the need to minimize panic, and the desire for full and accurate disclosure of material risks to the public?
- Does the Commonwealth, and its regional and local governments, have the public information capability to handle citizen inquires on homeland security and emergency matters (such as telephone hotlines, websites) and the ability to expeditiously respond to inquiries?
- How many of Virginia's citizens are aware of the steps citizens are advised to take in connection with different terrorist threat conditions (as set forth at http://www.commonwealthpreparedness.virginia.gov/SecureVa/vathreat.cfm)

and the need to develop an all hazards family disaster plan and disaster supply kit?

- Does the Commonwealth have a plan to increase overall public awareness of its plans and the steps the public should take?
    - Does the Commonwealth have the capability (including public relations liaisons) and strategies in place to work with the media to educate the public on these issues?

<u>Comment</u>: Empirical evidence available to date suggests that improvement is warranted in the public awareness of the steps for citizens to take at different threat levels and to prepare themselves for all hazards. Accordingly, the need for a plan to improve awareness is built in as an element of the needed capability on public awareness. The Joint Information Center ("JIC"), which is set up in the event of an emergency, should improve public awareness. However, efforts must be made to evaluate the overall effectiveness of the Center and modify its mission and operating procedures when necessary.

XVII. <u>Public Health & Medical Preparedness</u>

Does the Commonwealth have the medical and health care related capabilities (trained personnel, medicines, health care facilities, and other resources of sufficient size, scope and numbers) to investigate, respond to, and contain a range of "all hazards" events that could harm public health?

<u>Sub-Elements:</u>

- Does the Commonwealth have in place the following capabilities, systems and capacities, including necessary funding, personnel and equipment:
    - <u>Planning/Preparedness</u>:
        - A statewide plan to address the public health effects of "all hazards" that encompasses the following elements:
            - identification and prioritization, on a risk basis, of the full range of potential public health events that could occur in the Commonwealth, including events involving mass fatalities;
            - the effective management of the public health aspects of such events and their aftermath and the expeditious and coordinated delivery of critical health and mental health services, including:
                - identifying clear lines of responsibility within state government for handling needed functions in such public health emergencies;
                - developing state and regional plans for "surge capacity" for public health,

            healthcare and behavioral health responses to all such events, including emergencies involving mass fatalities; and
            - plans for collaboration with hospitals, the medical community, behavioral health providers, long term care facilities, outpatient facilities, homecare agencies, and other health providers and professionals in responding to such events.
        - a statewide system for 24 hour/7 day a week notification and/or activation of the public health emergency response system;
        - a system and directory of volunteers who can provide assistance in public health, healthcare and behavioral health responses to all emergencies;
        - statewide plans and procedures for receipt and distribution of medications and supplies from the Strategic National Stockpile and plans at the state and local levels for the timely dispensing of antibiotics or vaccines to affected populations;
        - corresponding all hazard plans for the local health districts; and
    - managing and counseling (as appropriate) individuals who suffer post-traumatic stress disorder, which are typical of events that involve mass fatalities.

- <u>Epidemiology/Early Disease Identification</u>

    - The capability and systems to:

        - receive and evaluate urgent disease reports, including ensuring legal authority to require and receive reports and investigate as appropriate;
        - assure the timeliness and completeness of reportable disease surveillance systems for outbreaks of illness;
        - maintain links with animal surveillance systems and the animal health community to facilitate identification and management of human diseases acquired from animals;
        - sufficient epidemiologic response capacity and capability to investigate and respond to infectious disease outbreaks, bioterrorism events, intentional or unintentional chemical exposures, radiologic events and natural emergencies that impact the health of the affected population; and
        - guidelines for implementing isolation and/or quarantine procedures as appropriate and necessary for individuals or populations.

- Laboratory Capability & Response

  - The capability and systems for:

    - rapid laboratory testing, with appropriate confirmation of results, for samples linked to infectious disease outbreaks, possible bio-terrorism events and chemical exposures, whether accidental or intentional;
    - rapid and safe transportation of samples to the laboratory for appropriate biologic or chemical testing; and
    - expedited communications between the state laboratory and the Virginia Department of Health, hospitals, other healthcare providers, and laboratories statewide for transmission of laboratory results.

- Communications/Information Technology

  - The capability and systems for:
    - notification of key stakeholders involved in public health or healthcare detection and response. including a 24 hour/7 day flow of critical health information;
    - redundant communications for public health and healthcare providers; and
    - coordination of communications and communications systems with all other emergency response agencies and organizations within the Commonwealth.

- Public Health Information

  - A plan for crisis and emergency risk communication and information dissemination concerning public health and healthcare issues;
  - training of key state & local public health spokespersons in crisis and emergency risk communication principles and standards;
  - coordination of risk communication planning, i.e. plans for communicating information to the media and the public during an emergency, with key state and local government and non-government emergency response partners;
  - collaboration of Commonwealth public health entities with Virginia's non-health emergency management units not only through the Joint Information Center, but also with input from the Emergency Operations Center, and the Fusion Center in order to assure coordinated communications with the media and public during any emergency event.

- Education and Training

  - Training for health department staff and healthcare providers in public health and healthcare emergency response to natural and man-made emergencies, including infectious disease outbreaks, terrorist events, chemical exposures, and radiological, nuclear, and explosive events. Training should include Incident Command, the National Incident Management System ("NIMS"), a DHS program that integrates practices in emergency preparedness and response into a comprehensive national framework for incident management, and the roles of all response agencies in responding to emergency events;
  - Coordination of training activities with all other state agencies involved in emergency response; and
  - Provision of access to necessary training to the broadest group of public health and private heath care providers, as well as other emergency responders (using newer technologies, where possible, to facilitate training)

Comment: To achieve the necessary level of public health planning, the Commonwealth needs to complete the preparation of its emergency operation plan ("EOP") and associated Emergency Support Function (ESF) 8 - the health and medical response emergency support function - consolidate all existing plans (SNS, smallpox pre-event and post-event, pandemic flu, SARS, etc.) within the EOP, and incorporate additional disaster and emergency plans as appropriate.

While various federal grants establish initial levels of surge capacity and related metrics (hospital beds per population size, etc.), there appears to be little empirical basis at present for identifying hard and fast levels of capability for the Commonwealth. Only continued exercises and experience will allow the development of more meaningful quantitative metrics for Virginia and its regions and localities. In developing these more measurable statistics, it also should be recognized that such metrics will likely change from one region to another (nationally and within states) and that a critical element is identifying state-wide metrics that rely heavily on transportation and mutual aid for surge capacity.

It should be recognized that few, if any jurisdictions are likely to have the range of capabilities noted above and that the Commonwealth, like other states, is now in the process of moving to acquire and make operational these types of capabilities.

Finally, as noted above, the public health capability of the Commonwealth has an emerging regional component that should be further developed and measured. The Virginia Department of Health ("VDH") has five regions for emergency planning and response (based on public health and healthcare planning and referral patterns) that are different from administrative regions utilized by the

Virginia Department of Emergency Management and the state police. The VDH effort includes a team of 5-6 people in each region as well as a hospital coordinator funded through federal grants that are involved in regional planning efforts and assisting health districts and hospitals in their regions. During emergencies, the regional teams assist the districts, hospitals, and VDH Central Office in collecting information and providing additional staff to districts most impacted by emergencies. These teams have only existed since late 2002-early 2003 and their roles are still evolving, but they have played major roles in regional planning and response to emergencies, including outbreak situations.

XVIII. Recovery

Does the Commonwealth, and its regions and localities, have the capability to timely recover from homeland security incidents and natural disasters?

Sub-Elements:

- Are recovery plans flexible to take into account the full range of threats and consequences?
- Do recovery plans establish priorities for the recovery effort, address the costs associated with recovery and the time frame for restoration of services, facilities, programs, and infrastructure?
- To what extent can the private sector and volunteer groups participate in recovery activities pursuant to an emergency situation?

Comment: Through recent disasters (including hurricanes Floyd and Isabel), Virginia has incorporated continuous improvement mechanisms into this process.

XIX. Training & Exercises

Training. Do the Commonwealth and its local governments regularly assess their training needs, and develop and implement a training/educational program for public/private officials and emergency response personnel?

Sub-Elements:

- Has the entity performed an assessment of training needs and develop and implemented a training/educational program to support the program?
    - Does the training and education program comply with all applicable regulatory requirements?
    - Is the training of emergency management personnel and key public officials given high priority?
- Does the training contribute to awareness and enhance the skills required to develop, implement, maintain, and execute the program?
    - Do emergency personnel receive and maintain training consistent with their current and potential responsibilities? (This includes, for

example, attendance at training events, conferences, workshops, exercises, seminars, and courses including formal education and degree programs where practical and feasible.)
    - Is specialized training sought in areas related to threats confronting the jurisdiction?
    - Is awareness training and education of key officials provided?
- Is the frequency and scope of the training identified in the program?
    - Is training regularly scheduled and conducted in conjunction with the overall goals and objectives of the training program?
    - Is the scope of training consistent with the training needs assessment?
    - Is the training related to correct action program deficiencies where possible?
- Are personnel trained on the entity's incident management system?
    - Do all emergency personnel undergo training on the incident management system of the program, including awareness of the operating systems of federal, state and local government, first responder and volunteer organizations?
- Are records maintained documenting training conducted?
    - Do the training program records include the names of those who have received training, the types of training planned and conducted, and qualifications of trainers?

Exercises. Does the Commonwealth have in place a robust exercise program for testing and evaluating its preparedness and the preparedness of its local governments?

Sub-Elements:

- Is the Commonwealth, and its local governments, periodically conducting the full range of exercises (discussion and operations-based) to test their preparedness?
    - How often have Commonwealth exercises been undertaken, and how many exercises have been completed at the local level per year (in absolute and percentage terms)?
- Are the exercises conducted in accordance with DHS Homeland Security Exercise and Evaluation Program (HSEEP) guidance and NFPA 1600 Standards § 5.13?
- Are the exercises multi-disciplinary and multi-agency?
- Do the exercises’ scenarios reflect potential threats and vulnerabilities?
- Do the exercises range in scope and increase in complexity over time?
- Does the Commonwealth or local government have an effective process to evaluate the results of the exercises, including the identification of capability areas where: 1) existing strengths are validated; and 2) improvements warranted.

  - Does the political subdivision have an improvement plan by which lessons learned from an exercise are turned into concrete, measurable steps that result in improved response capabilities?

Comment: In concert with DHS's Emergency Management Institute (EMI) program of resident and non-resident training, the Virginia Department of Emergency Management (VDEM) coordinates a wide variety training courses in five major programs: Emergency Management, Hazardous Materials, Radiological Emergency Response, Public Safety Response to Terrorism, and Search and Rescue. The efficient and effective training of first responders, state and local government officials, volunteer organizations, and the public and private sectors is key to the Commonwealth's ability to minimize the impact of disasters on its residents. Individual training provides the critical link that bonds policies and procedures, organizations, and equipment together that will contribute to a "safe, secure, and prepared Virginia."

Exercises are a key element of capability and performance measures because they refine needed capabilities and determine future performance measures. How is information gained from exercises acted upon?

As a component of the Commonwealth's comprehensive exercise program (CEP), the evaluation and assessment of exercises to validate strengths and identify improvement opportunities for the key response nodes/elements are critical for the state to meet its preparedness goals. The measurement of performance against a comprehensive, objective and straightforward set of criteria will provide those participating in training events with the most accurate assessment of their performance. While it may take time for organizations and jurisdictions to fully develop and practice their capabilities, the experience and incorporation of the "best practices" learned from a cycle of exercise activity conducted regularly will contribute significantly to achieving their preparedness objectives.

XX. Transportation

Are the Commonwealth's airports, bus and train stations, ports, bridges, rail lines, roads and highways and tunnels for carriage of persons and cargo ("transportation infrastructure" or "assets") sufficiently secure and are there plans and procedures in place to deal with potential threats to such critical transport assets in the event of a homeland security emergency, man-made accident, or natural disaster?

Sub-Elements:

- Have all such transportation assets been inventoried by the appropriate governmental entity and reviewed as part of the risk assessment process set forth above?

- Have all such transportation assets, whether publicly or privately owned and whether open to public or private transport, been legally licensed or registered in accordance with Commonwealth laws and regulations?
- Have all privately owned aircraft and other vehicles and vessels utilized in Virginia been registered or licensed in the state in accordance with Commonwealth laws and regulations?
- Have all such transportation assets developed, implemented, and funded preparedness plans that include elements on: physical and perimeter security; screening of passengers and luggage as appropriate; information security; coordination with local government and Commonwealth governmental authorities on issues that arise; and response to and recovery from man-made and natural disasters?
- Has the Commonwealth conducted or planned to conduct a study to systemically understand and address the interdependencies of transportation infrastructures with other infrastructures and systems of the Commonwealth, with respect to homeland security?
- Have the complementary roles of the responsible transportation agencies, including the Virginia Department of Transportation ("VDOT"), the Virginia Department of Rail and Port Transportation ("VDRPT"), the Virginia Port Authority ("VPA"), the Department of Aviation ("DOAV"), and the Department of Motor Vehicles ("DMV"), been adequately defined?
- Have the transportation providers in the private sector (e.g., Virginia Railway Express, airport commissions) been involved adequately in planning for Commonwealth preparedness?
- Have Commonwealth travelers, including private citizens and commercial vehicle operators, been adequately prepared to help prevent, respond, and recover from man-made and natural hazards to the transportation infrastructure?
- Have priorities for investments in transportation security been developed systematically and designed for maximum efficacy for the level of investment?

Comment: Developing and maintaining transportation security is a difficult, but important priority over the long-term. While some of the effort involves establishing appropriate procedures, other elements must rely on new and emerging technology that enable the detection of threats at transportation assets. New sensors and systems are under development and should be inserted into existing systems as expeditiously as possible.

In various transportation areas, the Commonwealth has developed and implemented plans. For example, the Virginia Area Maritime Security Committee ("AMSC") Circular No. 05-04 promulgates the Virginia Area Maritime Security Plan. The Maritime Transportation Security Act designated the Captain of the Port ("COTP") as the Federal Maritime Security Coordinator ("FMSC"). There are separate AMSC's for the National Capitol Region and Hampton Roads. Each respective FMSC has developed an Area Maritime

Security ("AMS") Plan covering areas of responsibility. The plans are designed as a port-wide command and control plan to deter and respond to Transportation Security incidents ("TSI"). Plans are developed in consultation with the AMSC and key maritime stakeholders. As the national and regional guidance for many of the complicated issues touched by the plan continue to be refined, changes and lessons learned will be incorporated.

Conclusion

In sum, the performance measures set forth above are a beginning, and not an end point. These measures – generally in question form – are designed to ascertain what plans, procedures, and, more fundamentally, core capabilities have been put in place. They should be vetted by expert groups and other stakeholders, fleshed out in more detail, and supplemented with a greater degree of numeric or specific standards where possible and appropriate. As noted earlier in the report, as time goes by and capabilities are put in place, the measures should focus less on the "existence" of capabilities and more on their effectiveness.

The utility of the performance measures or standards delineated herein will, of course, ultimately be found in terms of their incorporation into a performance measurement program implemented by the Commonwealth. The task force therefore recommends that such a performance measure program be initiated, possibly under the auspices of the OCP with assistance from the Panel. The result should be a Performance Measurement Program that draws upon the measures set forth herein and builds in additional objective measures where possible. Understanding the scope and potential complexity of such a program, the task force recommends that program initially adopt a "crawl before you walk" approach, maximizing leverage on ongoing activities (e.g., exercise and training programs), and consider the possibility of selected "pilot" efforts. These "pilots" would be designed to both prototype the measurement process and to make early progress in high priority domains (e.g., inter-agency interactions in the National Capital Region).

Further, the task force submits the following recommendations for consideration by the Commonwealth in developing a Performance Measurement Program for its preparedness:

1. Assessment Time Frames, Methods, & After-Action Reports. Performance standards should not simply be a set of guidelines that collect dust on shelves. Hence, to ensure the standards are operational, the Commonwealth should establish a set of requirements for:

    - annual or bi-annual reviews of the Commonwealth and its local governments;
    - the use of a range of assessment methods, including periodic self-assessments, peer reviews (by other Virginia governments or other state governments), and assessments by the Commonwealth of local governments; and
    - a clear approach to establishing "after-action" reports in response to events and exercises with regard to performance measure assessments conducted, including a clear ranking or grading criteria (whether color coding or otherwise) that shows how well the government unit performed, an analysis of why the performance measures were not met (i.e., what barriers exist) and a process for follow up on recommendations to assess if needed actions have and have not been taken.

2. Linking Performance Measures to Funding. It is our recommendation that the performance of local governments be taken into account by the Commonwealth as a significant factor in allocating or distributing federal grants and other available state funds. Local governments are hereby put on notice of the prospect that their performance, including their management of grant funds (see Performance Measure V, "Grant Functions," above) will in the future be considered in grant and other funding allocations or appropriations made by the Commonwealth along with other relevant funding factors.

3. Minimum Performance Measures. At the "enterprise level," as the performance measures set forth herein are further refined and made more specific, it is our recommendation that consideration be given, in some areas, to establishing some "minimum" performance thresholds that must be met by various levels of government.

Public/Private Cooperation Task Force of the Secure Commonwealth Panel

****

Recommendations to The Secure Commonwealth Panel & The Office of the Governor - Commonwealth Preparedness

MAY 10, 2005

Table Of Contents

Members

Kay Goss, Chair
Senior Advisor for Homeland Security
Business Continuity and Emergency
Management Services
Electronic Data Systems Corp. (EDS)

The Honorable Eugene J. Huang
Secretary of Technology

Robert P. Crouch, Jr.
Chief Deputy Secretary of Public Safety,

Steven M. Mondul
State Director, Security & Emergency
Management
Department of Transportation

Tom Hassler
President, Virginia Emergency
Management Association
Jefferson Lab

Michael M. Cline
State Coordinator, Virginia Department
of Emergency Management

Frances L. Kernodle
President, Kernodle and Associates

Anne F. Thomson Reed
President, Acquisition Solutions, Inc.

Larry Smith
Emergency Services Director
Tappahanock, VA

Thomas C. Franklin, Ph.D
President/CEO, Universal Security
Technology Group

William L. Radcliff
Homeland Security Advisor for SAIC

Debra Yamanaka
Homeland Security Advisor for SRA

Mark Penn
Emergency Management Coordinator
City of Alexandria

Archibald C. Reid
Federal Emergency Management
Association, Retired

Introduction

Mission of the task force

Address issues regarding public/private partnerships for securing the Commonwealth's critical infrastructure.

Policy Issues

- *Determine how the Commonwealth, the Department of Homeland Security and other federal agencies can improve their working relationship in the area of critical infrastructure protection*
- *Improve communication between the public and private sectors on security and preparedness issues*
- *Improve public/private coordination on critical infrastructure emergency planning and exercises*
- *Ensure the business community, as a whole, is prepared for disasters*

Guiding Principles

When discussions of homeland security turn to the role, possibilities, and challenges of the private sector, they typically have turned to four major areas:

Challenge 1: Security Screening

> *For example, some private sector leaders helped defeat, a legislative provision by Congressman David Obey that would have mandated 100% screening on all cargo in the belly of a commercial airplane. They contended that this would be difficult, if not impossible, in the short term without putting some major bottlenecks into the global supply chain.*
>
> *Yet, they know that we should be pushing for new tools and technologies to enhance cargo screening. Private sector's approach is that we should not impose new cost burdens on industry, which already pays billions of dollars in security user fees, 16 billion dollars at seaports alone.*
>
> *Private sector advocates that we adopt a well thought out and strategic view toward securing our supply chain. We should spend time and money investigating new technologies, and assess what economic benefit they would provide, in addition to any promised security improvement.*

Challenge 2: SAFETY Act

Private sector believes generally that it is essential for DHS to fully implement the SAFETY Act, which provides liability protections for private sector firms to deploy technologies that might otherwise not be broadly available, so that private sector innovators would have an incentive to take risks and put new anti-terrorism technology in the field quickly. DHS has been slow to certify technologies and services for SAFETY Act, but recently we have seen some improvement.

Private sector would like for DHS to link specific procurements to SAFETY Act designation. We know that some parts of DHS, including the Transportation Security Administration (TSA), are in fact fighting to link some of their upcoming requests for proposals to the SAFETY Act—and a final decision has not been made.

Challenge 3: Information Sharing

There is a widespread perception in both the public and private sectors that federal authorities have a lot more information on threats and vulnerabilities than is currently being shared, and that we would all be a lot better off if it were in fact shared.

Some industries are making great headway in this regard. In the transportation world, the Highway Watch program is a good example of some creative thinking to address this challenge. It is one of several initiatives in information sharing that has arisen from the sector-specific Information Sharing and Analysis Centers (ISAC) model that is now operational as part of our nation's critical infrastructure protection effort.

Public and private sectors agree that the state, federal and local governments should increase the sharing of information with the private sectors.

While it is easy to say information sharing is a good idea, implementation, even within the federal government alone, is a challenge, as current events have demonstrated. Collaboration between governments at all levels and with the private sector will take years, will require cultural change within our intelligence community, and will by necessity be a system built on trust, which takes time to develop. But we all must work to promote an enhanced dialogue between governments at all levels and the private sector.

A critical part of this promotion is the necessary first step--setting up the legal framework that protects companies when they share information with the government. DHS has issued an interim rule to protect this information when it's voluntarily submitted to them, and we are hopeful that we will soon see a good final regulation that sets the foundation for robust information sharing.

As a complement to this first step, DHS is, we understand, drafting its thoughts on information requirements--that is, what information the government would like from the private sector. We hear again and again from those in government that our member companies have information that would be useful if only they would share it. From our perspective, we would like to get beyond this rhetoric to a little more detail so that we can find a path forward in this critical area.

Additionally, the private sector is beginning to advocate a government-wide re-assessment of how information is classified, and for what purpose. Far too often, we hear that information cannot be shared with our members because it is classified. From our perspective, we are in a new era where robust sharing of intelligence information must be the norm, not the exception. The private sector feels an obligation to help the government modernize its intelligence capacity and shift the mindset from one of keeping all information close to sharing it more broadly, as appropriate.

By taking all these steps--setting the legal framework for information sharing, establishing information requirements and re-assessing how information is classified with the goal of classifying less and sharing more--the private sector will be better able to connect those dots and meet the threat of terrorism head on as partners with the government.

Challenge 4: Cyber Security

The private sector is committed to increasing the awareness of cyber security throughout the business community, explaining cyber security in terms that all businesses understand.

While advances in information technology have brought tremendous productivity gains for businesses and information resources for everyone, these advances come with risks. The software that makes this information revolution possible operates based on a series of codes. An error in code affects the ability of the Internet in general, and your computer specifically, to operate. Humans make this code and all humans make mistakes.

On a larger scale, entire segments of our economy are dependent on the Internet. As a result, bad actors are constantly looking for ways to launch an attack that could cripple the economy by bringing the Internet to a halt. For example, much of our power grid and financial services depend on the Internet for daily business operations. Internet dependent technology also is used to track packages, run trains and control dams. Therein lies the daunting challenge; our economy is propelled by complex, imperfect technology, and the average user of that technology does not understand the threat, let alone how to protect against that threat.

For cyber security, unlike most of the other areas, there is no relatively simple regulatory or legislative solution. Technology simply advances too quickly. Instead, ultimately the market is better able to respond to cyber security challenges since market forces propel companies to be flexible, innovative and customer oriented. Regulations, in contrast, are reactive and constrictive.

The private sector counts on the market, believing it remains a powerful vehicle for increasing cyber security, but before this power is fully realized, we need to better inform consumers on why cyber security is an issue that matters to them. They will demand more secure products, and successful firms will deliver those products.

One step in this process is the development of a cyber security guide for small businesses. Created in conjunction with the Internet Security Alliance and others, this guide outlines 12 cost effective steps that resource limited small businesses can take to better secure their networks.

For those of you who are interested in downloading a copy of the guide, you can do so from the US Chamber of Commerce website http://www.uschamber.com/default.

Raising awareness is not the only solution to enhancing cyber security. Instead, it is one part of the solution. Enhancing cyber security requires the combined efforts of users, systems engineers, technologists, and senior executives; those that use software and hardware, those that make software and hardware, and those who manage enterprises that rely on software and hardware to make the company operate. While technologists have a responsibility to make secure products, end users have a responsibility to use those products securely. Cyber security is everyone's problem and everyone can contribute to the solution.

Finally, the challenges facing our nation and our Commonwealth generally are daunting; but they are not insurmountable by any means. We can enhance our nation's homeland security while also continuing to have a global supply chain that moves goods effectively, efficiently, and with the speed we are used to. It will take hard work. It will take patience. And it will take a commitment by both the public and private sectors to make policy choices as partners who need one another to succeed.

The Commonwealth's Task Force on Public Private Cooperation in Homeland Security has attempted to set out some ways in which we can take our homeland security preparedness to a new and higher level, establishing a national model for other states in close public private cooperation. These recommendations are below.

Recommendations

I. Policy

Communications

The public and private sectors must increase their willingness and ability to share information, as this is vital to ensuring the cooperation needed to protect Virginia's critical infrastructure.

Issue 1 - Increase private sector awareness and access to government information.

Recommendations

1. The public and private sectors should work together to establish protocol for information sharing to protect private industry data.

2. There is state and federal law dealing with non-Freedom of Information Act (FOIA) status of Critical Infrastructure Information (CII). Part of the problem is that industry does not trust the government's ability to withstand legal attacks on this statute. Thus, government must work with business to build up the trust necessary for information sharing.

Business Preparedness

The private sector owns and operates 80-90% of critical infrastructure, hence, it is imperative that businesses be prepared for any risk and that the Commonwealth work with Virginia's businesses to assist their efforts.

Issue 1 - Businesses should develop emergency plans for any disaster, both man-made and natural.

Recommendations

1. Business should be prepared for disasters ranging from terrorist attacks to natural disasters to IT failures.

2. The Commonwealth's emergency plans should recognize that, while law enforcement is a key aspect of preparedness and security, it is vital to include members of the private sector, health experts, and other areas in the planning process, thus ensuring a comprehensive approach to preparedness.

3. One or more members of this task force should work to develop a template for the private sector (with special consideration of small business) that would feature "Five Easy Steps to Emergency Preparedness." The template could be refined by the full task force and submitted to the state for publication on its

website. The Commonwealth could print this plan in-house cost-efficiently and distribute it statewide through community offices of emergency preparedness or through local chambers of commerce.

Also, "Five Easy Steps to Emergency Preparedness" could be one of the information sheets inserted in packages for new business owners in Virginia communities and distributed by the Commonwealth when companies certify in any of the special initiatives, including certifications through the Dept. of Minority Business Enterprise and the Virginia Department of Business Assistance.

In addition, this information sheet could be a part of any package that is prepared for seminars or workshops that may evolve as a result of these recommendations. Incidentally, the task force recommends that using the term "emergency preparedness" rather than "security" as the word "security" is too widely used.

Defining the Threat

The public and private sector should need to know what threats Virginia's critical infrastructure face.

Issue 1 - To best prepare for threats there should be agreement between the public and private sector on which areas of critical infrastructure need the most improvement in emergency preparedness.

Recommendations

1. The public and private sector should work to develop a common list of threats to Virginia's critical infrastructure, as well as which infrastructure require additional emergency preparation.

2. Both sectors also need to develop a common definition of threat and what level of preparedness is satisfactory to meet the threats critical infrastructure faces in Virginia.

3. Both sectors should identify when public resources will be used to protect private assets during times of high alert.

Disaster Response Coordination

The public and private sector need to have a coordinated response plan for disasters, thus ensuring the most efficient response and recovery possible.

Issue 1 - How do we successfully leverage the multitude of skilled volunteers from the private sector to respond to a disaster?

Recommendations

1. The public and private sectors should develop mutual aid agreements and Memorandums of Understanding (MOU) for emergency volunteers.

2. The Virginia Department of Emergency Management should research this issue and work with a secretariat to develop legislation that would protect against lawsuits.

II. Process

Communications

The public and private sectors need to set up a communications process.

Issue 1 - Who will be the key players in communications between the public and private sectors?

Recommendations

1. Local government inspectors can serve as educators to local business because they already have a relationship and can provide information and assist in the businesses preparedness and security measures during annual visits.

2. The government can use local Chambers of Commerce, Rotary Clubs, and other local business organizations to market preparedness and security information as well as to disseminate information to smaller businesses during an emergency.

3. Governments can work with local business organizations to hold joint public/private conferences on preparedness and security.

4. The local emergency manager should serve as the "go to" person and coordinator during a disaster.

Issue 2 - Improve working relationship between the Commonwealth and DHS in the areas of critical infrastructure.

Recommendation

The Commonwealth should develop a stronger dedicated coordination structure to ensure coordination with DHS.

Identify Vulnerabilities

The public and private sectors need to work together to assess threat and prepare for emergency response.

Issue 1 - Ensure the business community, as a whole, is prepared for disasters.

Recommendations

1. The Commonwealth should conduct preparedness assessments of local businesses and put a sticker in the window of the businesses that pass or meet a certain standard. DHS funding for this program would be helpful.
2. The Office of Commonwealth Preparedness (via the Virginia Department of Transportation) is doing risk assessment on those facilities identified on the DHS Critical Infrastructure list as well as some others. This list is under revision. Private Industry can use public domain guides to complete risk assessments as well. The Commonwealth should encourage this practice in the business community ---perhaps through the private security industry.

3. The Commonwealth should leverage risk assessments, studies, and surveys etc., already completed by other entities, and determine how it will share that information.

4. Governments should involve local businesses in tabletop exercises.

III. Implementation

Communications Framework

The public and private sectors need to designate how they will communicate on a regular basis and during emergency situations.

Issue 1 - The government needs to disseminate information to the business community effectively and efficiently.

Recommendations

1. Text messaging is an effective method to ensure private building security and agents stay informed during an incident. Building security is a valuable resource and can better coordinate efforts with local law enforcement when responding to a disaster, if kept up-to-speed on response actions.

2. The Commonwealth has to be prepared to consistently update information so the private sector can rely upon it at any time, via both a website and radio. * The Commonwealth could sponsor a program, like the one in Chesterfield, to give free weather radios to businesses that cannot afford one.

3. National Incident Management System (NIMS) is an established framework by which the private sector could communicate with law enforcement.

4. Use Virginia Information Security Exchange (VISE) to bring the key government and private sector preparedness and security officials together to communicate.

5. The Fusion Center will foster the convergence of the cyber and physical ambit (enabler to monitor, manage, control and report on the connected elements within the entire system all within a single, integrated, common operating environment).
6. Government can partner with the media to disseminate information to the business community.

Issue 2 - What are the telecommunications requirements to ensure continuous, uninterrupted flow of information, during a disaster?

Recommendations

1. Consider VoIP - Voice over IP- a major step in the evolution of rich multimedia communications for businesses and consumers that are more personal, better integrated, and deliver better value to communications.

2. The local, state, and federal governments should cooperate to ensure first responders are able to communicate during a disaster. The government could work with the phone companies to have a line set aside for the first responders to use during a disaster.

Emergency Preparedness Information

To ensure the protection of critical infrastructure, businesses will need resources that provide the information they require to best prepare for disasters.

Issue 1 - Ensure the business community has the information and expertise it needs to best prepare for disasters.

Recommendations

1. Companies that have established plans and are prepared could serve as mentors to other businesses to teach them of how to best prepare for a disaster. The Commonwealth should encourage mentor protégé programs.

2. The state could host a best-practices website that would better educate businesses, particularly smaller businesses with limited resources, on how to best prepare for and recover from a disaster.

Conclusion

Nearly four years after the devastating attacks of 9/11, homeland security remains a top priority for national, state, and local leaders in the public and privates sectors throughout the nation. However, despite this heightened focus on our nation's and our Commonwealth's critical vulnerabilities, it is apparent that much more can and should be done to guarantee the protection of our citizens. Homeland security is a process, not a one-time event.

Our Commonwealth's business leaders must be better prepared to respond to threat to our security and should have a basic plan of action to inform and protect their employees and the citizens of their communities, as well as their facilities. Communication from government organizations, and public safety agencies to businesses, media, nonprofit organizations, volunteers and citizens should be clear and actionable.

Business leaders should be open to cooperation and collaboration at the Commonwealth and community levels, working to build strong public private partnerships that offer both government and business leaders the information, tools, and resources they need to meet their mutual interest in protecting the nation's vital infrastructure.

With 85% of the nation's critical infrastructure in the hands of the private sector, industry has an important role to play in the current environment. Accordingly, businesses have an opportunity to build stronger bonds with government and work together as partners in preparedness.